

Public Document Pack

Mid Devon District Council

Community Policy Development Group

Tuesday, 20 August 2019 at 2.15 pm
Exe Room, Phoenix House, Tiverton

Next ordinary meeting
Tuesday, 8 October 2019 at 2.15 pm

Those attending are advised that this meeting will be recorded

Membership

Cllr W Burke
Cllr Mrs C P Daw
Cllr J M Downes
Cllr Mrs I Hill
Cllr B Holdman
Cllr E G Luxton
Cllr Miss J Norton
Cllr C R Slade
Cllr Mrs M E Squires

A G E N D A

Members are reminded of the need to make declarations of interest prior to any discussion which may take place

- 1 **Apologies and Substitute Members**
To receive any apologies for absence and notices of appointment of substitute Members (if any).
- 2 **Declarations of Interest under the Code of Conduct**
Councillors are reminded of the requirement to declare any interest, including the type of interest, and reason for that interest, either at this stage of the meeting or as soon as they become aware of that interest.
- 3 **Public Question Time**
To receive any questions relating to items on the Agenda from members of the public and replies thereto.

Note: A maximum of 30 minutes is allowed for this item.
- 4 **Minutes of the Previous Meeting** (*Pages 5 - 10*)
Members to consider whether to approve the Minutes of the meetings held on 25th June 2019.

The committee is reminded that only those Members present at the

previous meeting should vote and, in doing so, should be influenced only by seeking to ensure that the minutes are an accurate record

5 **Chairmans Announcements**

To receive any announcements that the Chairman may wish to make.

6 **Cabinet Member for Community Wellbeing** (*Pages 11 - 14*)

To receive a report of the Cabinet Member for Community Wellbeing on areas within his remit.

7 **Performance & Risk** (*Pages 15 - 24*)

To provide members with any update on performance against the corporate plan and local service targets for 2019/2020 as well as providing an update on the key business risks.

Note: The Leisure performance reports are restricted.

8 **CCTV Annual Update** (*Pages 25 - 58*)

To update Members on the Town Centre CCTV system and operational overview from the Group Manager for Corporate Property and Commercial Assets

9 **CTF Fund Summary 2018-2019** (*Pages 59 - 66*)

To receive a report on the Communities Together Fund for 2018-2019 from the Group Manager for Growth, Economy and Delivery

10 **Regulation of Investigatory Powers** (*Pages 67 - 90*)

To receive the annual review of Regulation of Investigatory Powers Policy from the Director of Corporate Affairs and Business Transformation.

11 **Public Health Update**

To receive an overview of the Public Health Department and how this relates to the work of the Policy Development Group from the Group Manager for Public Health and Regulatory Services

12 **Identification of Items for the Next Meeting**

Please note the following items have been identified for future meetings:

Single Equalities Policy and Equality Objective

Air Quality Action Plan Update

Financial Monitoring

Community Safety Partnership

Strategic Grants and Service Level Agreement Programme 2020-2023

Training Opportunities

Note: This item is limited to 10 minutes. There should be no discussion on the items raised.

Stephen Walford
Chief Executive
Monday, 12 August 2019

Anyone wishing to film part or all of the proceedings may do so unless the press and public are excluded for that part of the meeting or there is good reason not to do so, as directed by the Chairman. Any filming must be done as unobtrusively as possible from a single fixed position without the use of any additional lighting; focusing only on those actively participating in the meeting and having regard also to the wishes of any member of the public present who may not wish to be filmed. As a matter of courtesy, anyone wishing to film proceedings is asked to advise the Chairman or the Member Services Officer in attendance so that all those present may be made aware that is happening.

Members of the public may also use other forms of social media to report on proceedings at this meeting.

Members of the public are welcome to attend the meeting and listen to discussion. Lift access the first floor of the building is available from the main ground floor entrance. Toilet facilities, with wheelchair access, are also available. There is time set aside at the beginning of the meeting to allow the public to ask questions.

An induction loop operates to enhance sound for anyone wearing a hearing aid or using a transmitter. If you require any further information, or

If you would like a copy of the Agenda in another format (for example in large print) please contact Carole Oliphant on:

Tel: 01884 234209

E-Mail: coliphant@middevon.gov.uk

Public Wi-Fi is available in all meeting rooms.

This page is intentionally left blank

MID DEVON DISTRICT COUNCIL

MINUTES of a **MEETING** of the **COMMUNITY POLICY DEVELOPMENT GROUP**
held on 25 June 2019 at 2.15 pm

Present Councillors

W Burke, J M Downes, Mrs I Hill,
E G Luxton, C R Slade, Mrs M E Squires,
L J Cruwys and B A Moore

Apologies Councillor(s)

Mrs C P Daw, B Holdman and Miss J Norton

Also Present Councillor(s)

R J Chesterton and D J Knowles

Also Present Officer(s):

Andrew Jarrett (Deputy Chief Executive (S151)), Kathryn Tebbey (Group Manager for Legal Services and Monitoring Officer), Simon Newcombe (Group Manager for Public Health and Regulatory Services), Catherine Yandle (Group Manager for Performance, Governance and Data Security), Rob Fish (Principal Accountant), Corinne Parnall (Leisure Manager - Health & Fitness) and Sally Gabriel (Member Services Manager)

1 ELECTION OF CHAIRMAN (THE CHAIRMAN OF THE COUNCIL IN THE CHAIR)

RESOLVED that Cllr C R Slade be elected Chairman for the municipal year 2019-2020.

2 ELECTION OF VICE CHAIRMAN (00-01-32)

RESOLVED that Cllr B Holdman (in his absence) be elected Vice-Chairman of the Committee for the municipal year 2019/20.

3 APOLOGIES AND SUBSTITUTE MEMBERS (00-02-33)

Apologies were received from Cllr Mrs C P Daw who was substituted by Cllr B A Moore and from Cllr B Holdman who was substituted by Cllr L J Cruwys.

4 DECLARATIONS OF INTEREST UNDER THE CODE OF CONDUCT

Cllrs Mrs I Hill and B A Moore declared personal interests with regard to Item 9 (6 Month Leisure Update) as they held Zest Cards.

5 PUBLIC QUESTION TIME

There were no members of the public present.

6 MINUTES OF THE PREVIOUS MEETINGS

Due to the new administration, the minutes of the previous meetings were noted.

7 CHAIRMANS ANNOUNCEMENTS

The Chairman thanked the Group for electing him as Chairman and following the recent press release with regard to food inspection congratulated the Environmental Health Team for their hard work.

8 GRANT FUNDED AGENCY

Alison Padfield (Manager) from CHAT (Churches Housing Action Team) gave an overview by way of presentation on the work of the organisation. She explained that the organisation had been established for 24 years, had a team of 10 staff with 20 volunteers and worked across the whole of Mid Devon. She outlined the areas that the organisation focussed on which was primarily tenancy support, housing advice and debt and money advice.

Emergency help was provided for those in need which included:

- The foodbank, which was generously supported by the local community and referrals were made to the organisation from outside agencies which included Social Services, AGE UK, Citizens Advice, GP's , the job centre and schools.
- Hardship – mobile phones, home start up kits, travel and tents were made available
- The Fuel Poverty Fund – £2045 had been granted
- A warm welcome – the use of showers, clothes washing facilities and somewhere safe to be

She outlined the number of clients in the previous year and the general statistics available, the work of the volunteers, the fund raising that had taken place and the plans for the future.

Discussion took place regarding:

- The grant funding supplied by the District Council
- The impact of Universal Credit
- The work taking place in rural areas and how Councillors could raise awareness of the organisation
- How much the service was welcomed and the good work that it did

The Chairman thanked Mrs Padfield for her attendance.

9 6 MONTH LEISURE UPDATE (00-26-30)

The Leisure Manager gave the Group an update by way of a presentation highlighting the work of the Leisure Team and the number of staff (186 team members with 60 FTE) across the 3 leisure facilities at Exe Valley, Culm Valley and Lords Meadow which operated for 106 hours per week and 362 days of the year. In the last financial year 894,329 visits had been made to the facilities.

She explained the partnership work and health and wellbeing initiatives taking place on both the wet and dry side of the facilities and the GP referral scheme for specific rehabilitation that was also taking place.

She provided photographs of each site and explained the refurbishment that had taken place and the work that was proposed for the future.

The Chairman thanked the Leisure Manager for her presentation and update.

Notes:

- i) Cllrs Mrs I Hill and B A Moore declared personal interests as they both held Zest Cards;
- ii) *Report previously circulated, copy attached to minutes.

10 MOTION 554 (COUNCILLOR R J CHESTERTON - 20 MARCH 2019) (00-46-52)

At its meeting on 24 April 2019, Council had referred the following Motion to the Community Policy Development Group for its consideration.

Motion 554 (Councillor R J Chesterton - 20 March 2019)

Parish and town councils should, in reply to any street naming proposal from a developer, be allowed to recommend to this Council that a street be named after an individual, including the living.

The Group had before it a report* of the Group Manager for Legal Services for consideration. She outlined the contents of the report explaining the procedure in place, the guidance that was available, the possible implications of naming a street after a living person and how other Devon authorities dealt with the matter. She highlighted in particular the guidance from Plymouth City Council.

Cllr Chesterton explained the reasoning behind his motion as he felt there was a desire to name streets after people who had achieved something in their lifetime and that this should be recognised whilst they were still alive.

Consideration was given to:

- Achievements could be forgotten and naming a street after a particular person would be well received
- The need for the local community to approve any proposal and the consultation process that took place
- The checks and balances that would have to be in place prior to any recommendation

It was therefore

RECOMMENDED to Council that Motion 554 be supported.

The Policy Development Group also recommended that the following wording be placed in the Council's procedure:

In exceptional circumstances should a proposal be made to name a Street after a living individual, on the grounds of them having made an outstanding contribution to the locality and/or its people, these will be permitted if both approval by the individual and unanimous agreement between the Cabinet Member with delegated authority for the service and appropriate Ward members is received.

(Proposed by the Chairman)

Note *Report previously circulated, copy attached to minutes.

11 REVENUE AND OUTTURN REPORT (1-01-09)

The Group had before it and **NOTED** a *report of the Deputy Chief Executive (S151) presenting the Revenue and Capital Outturn report for 2018/19. He outlined the contents of the report informing the meeting of the following highlights

- The final monitoring report presented to the Group prior to the election had predicted an end of year deficit of £65k for the General Fund. However, the final position had improved by £84k meaning that the General Fund for 2018/19 would finish with an underspend of £19k
- In year financial monitoring throughout 2018/19 had been very accurate.
- It had been possible to set aside funds to Earmarked Reserves where needed.
- The recommendation to the Cabinet to carry forward circa £12m from the 2018/19 capital programme to fund schemes in the years to come. In addition to this the recommendation to transfer to earmarked reserves £459k which had been unspent.
- The positive position of the HRA which showed a saving of £613k and the transfer of the same to earmarked reserves.
- The Collection Fund and how effective the Revenues section had been in collecting Council Tax and NNDR during extremely challenging economic times
- Market Walk and Fore Street shops in Tiverton. There had been a number of voids throughout the year but in December 2018 every unit in Market Walk had been occupied although overall rents had been lower.

The Principal Accountant provided detailed information of the outturn for the specific budgets under the remit of the Group highlighting the major variances within the report.

Consideration was given to:

- The underspend on the Capital Programme and which projects had slipped and when they would be progressed
- Funding for the Garden Village
- Remittances received via Planning S106 agreements.
- Whether variances could be depicted minus the additional windfalls so that a clearer picture could be identified

Note *Report previously circulated, copy attached to minutes.

12 **PERFORMANCE & RISK (1-29-24)**

The Group had before it and **NOTED** a *report of the Group Manager for Performance, Governance and Data Security regarding the Outturn performance against the corporate plan and local service targets for 2018/2019.

The officer outlined the contents of the report highlighting the total refurbishment of the fitness studio at Lords Meadow, the completion of the trim trail at Amory Park, the compliance with food safety law, the announcement by Gigaclear regarding the delay in delivering superfast broadband across Devon and the digital inclusion work that had commenced.

Consideration was given to:

- The record number of food inspections that had taken
- With regard to scores on the doors, over 96% of food establishments were good or very good.
- The on-going risk of cyber security

Note: *Report previously circulated, copy attached to minutes.

13 **START TIME OF MEETINGS (1-38-04)**

It was agreed that the Group would continue to meet at 2.15pm for the remainder of the municipal year.

14 **IDENTIFICATION OF ITEMS FOR THE NEXT MEETING (1-39-00)**

There were additional items proposed to the work programme.

(The meeting ended at 3.55 pm)

CHAIRMAN

This page is intentionally left blank

COMMUNITY PDG 20 August 2019

UPDATE REPORT OF CABINET MEMBER FOR COMMUNITY PDG

Cabinet Member: Cllr Dennis Knows
Responsible Officer: Various

Reason for the report: to update members on progress within those services that fall within the community portfolio.

Strategic Grants:

- The Council continues to fund a small number of community organisations whose work is seen to be of strategic importance to the Council. These are Citizen's Advice, Churches Housing Action Team (CHAT), Mid Devon Mobility, Age Concern Mid Devon, and INVOLVE – Voluntary Action in Mid Devon. The three year agreements for these organisations are due for review this autumn, and a report will be coming to the Community PDG in October outlining the process for reviewing funding for April 2020 onwards.

ICT Services:

- New 3 year Microsoft Enterprise Agreement started July 2019, this includes licenses for Office 365 and Enterprise Voice, which will enable MDDC to move to a Unified Communications platform in the near future.
- Phase 1 of the workstation refresh deployment is currently under way, replacing a mix of pc's, laptops and monitors.
- All desktop\laptop Operating Systems are being upgraded to Windows 10, this will need to be completed by the end of this calendar year as current system (Windows 7) has reached the end of support and can no longer be used.
- Completed replacement of all the Uninterruptible Power Supplies (UPS) which are used to ensure a 'clean' electrical supply to ICT Infrastructure hardware and provide short term power resilience.
- A major server and storage replacement project will take place during August – September, which will include Email servers, Virtual Server environment, Corporate SQL Database Server and shared drives. This refresh will provide improved system performance and capacity.

Gazetteer Management Services:

- Continue to maintain the gazetteer to a high standard achieving Gold at a national level and providing daily change updates to the national hub, thus ensuring our entitlement to the supply of "free at point of use" OS mapping data
- Continue to maintain property links to non-Uniform systems in the authority helping to ensure the integrity of associated data
- Continue the role out of QGIS as an open source (free) supplementary mapping system to the corporate ESRI ArcGIS software, widening the availability of spatial data to more officers in the authority

- Work towards the completion of the updating of the authority's property ownership database

Land Charges:

- The Group Manager for Legal Services and Monitoring Officer has overall responsibility for the Land Charges team, although day-to-day management is carried out by Pauline Davey, Senior Local Land Charges Officer. The team is also responsible for street naming and numbering.
- The national programme of transferring land charges data to the Land Registry continues as part of a phased programme. The final aim is to create a new digital local land charges service through the Land Registry. However, local authorities will continue to be responsible for certain types of enquiries (CON29) and will have to deal with enquiries about the detail or accuracy of any data obtained from the Land Registry. It is fair to say that there is therefore some scepticism amongst practitioners and conveyancers as to the benefits of the programme. So far, the local land charges data of only 6 local authorities has been transferred. Quite how long it will take to get to Mid Devon is unclear, but we are not in the programme for 2019. Our land charges team continues to carry out the usual land charges function whilst completing a number of tasks in preparation for migration of data.
- There is new burdens funding available for certain costs associated with the transfer and this would be established in an agreement between the local authority and the Land Registry and the start of the transfer process. The precise implications on staffing are currently unknown – a local land charges service will remain, but it may well require fewer staff resources. This will only become clear at or (more likely) following the transfer stage.
- The Land Charges team must also be congratulated for yet another national award nomination in 2019. The team of Pauline Davey and Donna Oswald were successful in 2016 and 2018, so this shows that they continue to deliver a service of a consistently high quality which is recognised by users of the service.

Leisure:

Front of House

- Membership and Sales Training carried out across site to continue to provide an excellent customer journey at all three sites.
- 100% response rate, 1 day response time for Facebook notifications
- New BACS procedure to implemented
- 'Mystery Shopper' programme continues

Wetside

- SWIMTAG remains popular amongst all ages with a total of 410 swimmers now signed up at EVLC
- LMLC hosted first Junior Duathlon event
- Re lining of the learner pool at EVLC completed
- LMLC pool maintenance project planned for winter 2019/20
- Sport England bid submitted for funding for SWIMTAG at LMLC

Health & Fitness

- Development of Lord's Meadow Leisure Centre Fitness studio
- New indoor cycle bikes arrived at LMLC and CVSC
- Re-branding and refurbishments of fitness studios at all three centres planned
- Pilot course for Arthritis care at EVLC
- NHS group for Parkinson's hiring LMLC Dance Studio.

Dryside

- CVSC refurbishment of sauna
- Tennis court enhancement at LMLC (they will retain the 4 tennis courts and have three new netball courts)
- "Kids who care" fun day, to be hosted at CVSC, conjunction with "Involve", Mid Devon on 15 August
- Hall curtain renewal at CVSC started

Public Health:

Commercial Team (food hygiene, health and safety, licensing and infectious diseases)

- Record number of inspections and other interventions at food premises 18-19 (1291 vs 554 in the previous year)
- Number of on-going enforcement cases including potential prosecutions for health and safety and food hygiene offences at two separate commercial premises
- Approval for updated taxi licensing policy (Hackney Carriage and Private Hire) including new provisions to make safeguarding training mandatory for all licensed drivers and introduce rolling 6-monthly disclosure and barring checks (DBS)
- Our work on regulating our taxi providers including vehicle checks recently received positive media recognition locally
- Licensing officers successfully completed mandatory animal premises inspection qualifications under new, enhanced animal licensing regime

Community Team (environmental protection only)

- Recently concluded joint-working with Public Health England regarding a long running 'prejudicial to health' investigation in the Templeton area
- Successfully completed annual Air Quality report for Defra and making key progress on delivery of measures in the Air Quality Action Plan for Crediton and Cullompton
- Introduced new noise app for the public to record evidence and submit complaint information via their smartphones
- Recently reported to Scrutiny Committee on a the positive delivery of our Community Safety Partnership Action Plan for 18-19 and looking ahead at new duties for the partnership to produce a joint violent crime strategy

Service lead level

- Completed a key emergency planning exercise to test the effectiveness of the MDDC Recovery Plan in the event of a major incident
- Successfully gained accreditation in investigative practice through completion of an Advanced Professional Certificate in Investigative Practice (APCIP)
- Introduced a new, comprehensive Operations Directorate Enforcement Policy underpinning the majority of the enforcement work undertaken by MDDC

Police and Crime Panel

I attended the police and crime panel at Plymouth, on the 14th June 2019. Which discussed the yearly report by Alison Hernandez, and afterwards had a small meeting to arrange a programme of items to be debated over the next year.

I laid before the committee the subject of police on our streets and the opening of local police stations.

As and when this is debated, I will report back.

Cllr Dennis Knowles
Cabinet Member for Community Wellbeing

COMMUNITY PDG 20 AUGUST 2019:

PERFORMANCE AND RISK FOR 2019-20

Cabinet Member Cllr Dennis Knowles
Responsible Officer Director of Corporate Affairs & Business Transformation,
Jill May

Reason for Report: To provide Members with an update on performance against the corporate plan and local service targets for 2019-20 as well as providing an update on the key business risks.

RECOMMENDATION: That the PDG reviews the Performance Indicators and Risks that are outlined in this report and feeds back areas of concern to the Cabinet.

Relationship to Corporate Plan: Corporate Plan priorities and targets are effectively maintained through the use of appropriate performance indicators and regular monitoring.

Financial Implications: None identified

Legal Implications: None

Risk Assessment: If performance is not monitored we may fail to meet our corporate and local service plan targets or to take appropriate corrective action where necessary. If key business risks are not identified and monitored they cannot be mitigated effectively.

Equality Impact Assessment: No equality issues identified for this report.

Impact on Climate Change: No impacts identified for this report.

1.0 Introduction

- 1.1 Appendix 1 provides Members with details of performance against the Corporate Plan and local service targets for the 2019-20 financial year. The PDG is invited to suggest measures they would like to see included in the future for consideration.
- 1.2 Appendix 2 shows the section of the Corporate Risk Register which relates to the Community Portfolio. See 3.0 below.
- 1.3 Appendix 3 shows the profile of all risks for the Community Portfolio.
- 1.4 The Community PDG agreed that the performance indicators for Leisure would be provided in Part II to allow Members to review performance without risk to the Leisure business. This information is included as Appendix 4
- 1.5 All appendices are produced from the corporate Service Performance And Risk Management system (SPAR).

2.0 Performance

2.1 **Regarding the Corporate Plan Aim: Promote physical activity, health and wellbeing:** The Council invested in the region of £10,000 to improve the existing tennis courts, at Lords Meadow in Crediton, making them multi-purpose for the use of netball as well as tennis. The improvement work was completed on budget.

2.2 The paddling pool in Westexe Park, Tiverton was reopened in time for the school summer holidays. A maintenance team has been recruited to carry out the additional workload which includes testing the pool water three times a day, seven days a week.

2.3 **Other:** The upgraded website went live on 1 July with accessibility changes. Mid Devon Matters; a quarterly newsletter was launched at the Mid Devon Show.

2.4 At a regulatory committee meeting the specialist lead licensing officer told members the Council had 121 licensed vehicles on its register, and 51 of those had been proactively inspected by enforcement officers.

2.5 MDDC has applied for £1.2 million of Government funding to support the regeneration of Cullompton's historic town centre. The Council submitted the bid to Historic England for a share of the High Streets Heritage Action Zone, under the Government's High Streets Programme. The bid is specific to Cullompton.

3.0 Risk

3.1 Risk reports to committees include strategic risks with a current score of 10 or more in accordance. (See Appendix 2)

3.2 Operational risk assessments are job specific and flow through to safe systems of work. These risks go to the Health and Safety Committee biannually with escalation to committees where serious concerns are raised.

3.3 The Corporate risk register is regularly reviewed by Group Managers' Team (GMT) and Leadership Team (LT) and updated as required.

4.0 Conclusion and Recommendation

4.1 That the PDG reviews the performance indicators and risks for 2019-20 that are outlined in this report and feedback any areas of concern to the Cabinet.

Contact for more Information: Catherine Yandle, Group Manager Performance, Governance and Data Security ext 4975

Circulation of the Report: Leadership Team and Cabinet Member

Corporate Plan PI Report Community

Monthly report for 2019-2020
Arranged by Aims
Filtered by Aim: Priorities Community
Filtered by Flag: Exclude: Corporate Plan Aims 2016 to 2020
For MDDC - Services

Key to Performance Status:

Performance Indicators:

No Data	Well below target	Below target	On target	Above target	Well above target
---------	-------------------	--------------	-----------	--------------	-------------------

* indicates that an entity is linked to the Aim by its parent Service

Corporate Plan PI Report Community

Priorities: Community

Aims: Other

Performance Indicators																	
Title	Prev Year (Period)	Prev Year End	Annual Target	Apr Act	May Act	Jun Act	Jul Act	Aug Act	Sep Act	Oct Act	Nov Act	Dec Act	Jan Act	Feb Act	Mar Act	Group Manager	Officer Notes
<u>Compliance with food safety law</u>	85% (3/12)		90%	93%	93%	92%										Simon Newcombe	

This page is intentionally left blank

Community PDG Risk Management Report - Appendix 2

Report for 2019-2020

For Community - Cllr Dennis Knowles Portfolio

Filtered by Flag:Include: * Corporate Risk Register

For MDDC - Services

Not Including Risk Child Projects records, Including Mitigating Action records

Key to Performance Status:

Mitigating Action:	Milestone Missed	Behind schedule	On / ahead of schedule	Completed and evaluated	No Data available
--------------------	-------------------------	------------------------	-------------------------------	--------------------------------	--------------------------

Risks:	No Data (0+)	High (15+)	Medium (6+)	Low (1+)
--------	---------------------	-------------------	--------------------	-----------------

Community PDG Risk Management Report - Appendix 2

Risk: Cyber Security Inadequate Cyber Security could lead to breaches of confidential information, damaged or corrupted data and ultimately Denial of Service. If the Council fails to have an effective ICT security strategy in place.

Risk of monetary penalties and fines, and legal action by affected parties

Service: I C T

Mitigating Action records

Mitigation Status	Mitigating Action	Info	Responsible Person	Date Identified	Last Review Date	Current Effectiveness of Actions
Completed and evaluated	Email and Protective DNS	ICT have applied the all levels of the government secure email policy, which ensures secure email exchange with government agencies operating at OFFICIAL. PSN DNS has been configured at the Internet gateway, which ensures the validity of websites and blocks known sites.	Alan Keates	06/06/2019	06/06/2019	Fully effective (1)
	Information Security	Information Security Policy	Catherine Yandle	22/10/2015	06/06/2019	Fully effective (1)

Community PDG Risk Management Report - Appendix 2

Mitigating Action records						
Mitigation Status	Mitigating Action	Info	Responsible Person	Date Identified	Last Review Date	Current Effectiveness of Actions
Completed and evaluated	Policy in place, with update training	reviewed. LMS (online policy system) included in induction.				
On / ahead of schedule	Regular user awareness training	Staff and Member updates help to reduce the risk	Alan Keates	03/01/2019	06/06/2019	Satisfactory (2)
Completed and evaluated	Technical controls in place	Required to maintain Public Sector Network certification	Alan Keates	03/01/2019	06/06/2019	Fully effective (1)
Current Status: High (20)		Current Risk Severity: 5 - Very High		Current Risk Likelihood: 4 - High		
Service Manager: Alan Keates						
<p>Review Note: ICT have applied the all levels of the government secure email policy, which ensures secure email exchange with government agencies operating at OFFICIAL. PSN DNS has been configured at the Internet gateway, which ensures the validity of websites and blocks known sites.</p>						

Risk: Health and Safety Inadequate Health and Safety Policies or Risk Assessments and decision-making could lead to Mid Devon failing to mitigate serious health and safety issues

Service: Human Resources

Mitigating Action records						
Mitigation Status	Mitigating Action	Info	Responsible Person	Date Identified	Last Review Date	Current Effectiveness of Actions
Completed and evaluated	Risk Assessments	Review risk assessments and procedures to ensure that we have robust arrangements in place. In progress ready for September reports.	Michael Lowe	28/05/2013	15/11/2018	Fully effective (1)
Current Status: Medium (10)		Current Risk Severity: 5 - Very High		Current Risk Likelihood: 2 - Low		
Service Manager: Michael Lowe						
<p>Review Note: Whilst there is an improvement in procedures the safety reviews carried out still show further work is required in implementing these into the work place</p>						

Risk Matrix Community Appendix 3

Report For Community - Cllr Dennis Knowles Portfolio Current settings

Risk Likelihood	5 - Very High	No Risks	No Risks	No Risks	No Risks	No Risks
	4 - High	No Risks	No Risks	No Risks	No Risks	1 Risk
	3 - Medium	No Risks	1 Risk	3 Risks	No Risks	No Risks
	2 - Low	No Risks	4 Risks	14 Risks	4 Risks	7 Risks
	1 - Very Low	1 Risk	No Risks	No Risks	3 Risks	2 Risks
	1 - Very Low	2 - Low	3 - Medium	4 - High	5 - Very High	
	Risk Severity					

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

**COMMUNITY PDG
20 AUGUST 2019
CCTV ANNUAL UPDATE**

Cabinet Member(s): Cllr Simon Clist.
Responsible Officer: Andrew Jarrett Deputy Chief Executive (151).

Reason for Report: To provide Members with an update to the Tiverton Town Centre CCTV system including an operational overview.

RECOMMENDATION: That members note the action plan attached as Annex A regarding the upgraded CCTV facilities and the benefits of the system to the Tiverton Community.

Financial Implications: The one off purchase and implementation of the CCTV System was funded by capital funds. The ongoing maintenance and servicing of the system is, however, a revenue cost which will be funded through the revenue budget partly offset by the financial contributions which are received annually from Tiverton Town Council. On occasions the police and community safety are also able to provide funding.

Legal Implications: As part of the action plan, see 7.0, the Council will conduct a review to consider whether or not to use a surveillance system and evaluate whether it is necessary and proportionate to continue using it. The Council will need to meet the latest practice requirements, which are attached to this report as Annex A. There are 15-16 signs around Tiverton displaying that member(s) of the public are being recorded on CCTV.

Risk Assessment: If the CCTV is not operating the police have less evidence to identify and pursue individuals who have been involved in criminal activities in the area, therefore crime could potentially rise. There is wider coverage of the town centre area and more incidents and criminal activity can be monitored and images provided to the police when required. The need will be assessed as part of the action plan review.

Equality Impact Assessment: No equality issues have been identified.

Relationship to Corporate Plan: Property services are committed to ensuring the wellbeing and safety of Mid Devon communities. The way that the Council manages the CCTV has a direct impact on the safety of the community so it is therefore important to ensure that the CCTV is operating correctly and efficiently.

Impact on Climate Change: The environmental impact is considered to be low, however the operation of the CCTV will be included when calculating our carbon footprint.

1.0 Introduction/Background

- 1.1 The Tiverton Town Centre CCTV is a discretionary service to which the Council has a limited budget to maintain the system. The monitoring of the CCTV system is based on a voluntary basis with additional hours when necessary to protect the Multi Story Car Park (MSCP), the Council pays the volunteer 7 hours per week towards the monitoring of the CCTV. The Tiverton Town Centre CCTV system is regularly used for crime prevention and improving community safety. The police service regularly contacts the CCTV volunteer to aid officers in policing activity. The Tiverton Town Centre CCTV was an initiative from June 2011 when a working member's group review of the CCTV led to some of the CCTV systems being upgraded during the 2016/17 financial year. Currently that investment means we have an operational system however repairs can be costly and are subject to vandalism that puts pressure on this discretionary service.
- 1.2 The CCTV system continues to be frequently used by the Tiverton Policing Team in liaison with the CCTV supervisor.

2.0 Tiverton Town Centre System

- 2.1 The system has a total of 26 cameras covering the Tiverton Town Centre and the Pannier Market area. In addition there are also some operational camera monitoring the entrances and exits of the MSCP, this monitoring area is likely to be upgraded under the MCSP improvement project once the tenders that have been received are evaluated.
- 2.2 When the system was upgraded in 2016 the Council consulted with the partner agencies including the Police, Highways and Devon County Council to identify the best location for the cameras to ensure the best possible coverage of the town centre key areas. These are areas where there is most public footfall or known hotspots for criminal activity and anti-social behaviour. Several of the cameras are radio linked so need to be in line of sight of others in order to transmit the images back to the control room. This needed careful planning in order to get the best possible vantage points.
- 2.3 The Council obtains permissions from the private property owners to install camera equipment on their premises and arranges for the power from nearby street furniture.
- 2.4 The CCTV control room has monitors and a larger hard drive to store the footage, for up to 30 days, from the cameras. Software is in use and the CCTV operator has had the relevant data protection training to view, retrieve and add footage to secure memory devices as required, by the Police Authority, following a strict protocol for chain of evidence.

3.0 CCTV Surveillance

- 3.1 The CCTV supervisor is employed for 7 hours per week; however he increases these hours considerably in a number of ways, additional hours to cover school and public holidays, police requests for weekend operations support and voluntary monitoring of the Town's CCTV systems. On average

the cameras are currently 'manned' in excess of 40 hours per week and this will most often include a Saturday evening / overnight. During busy periods such as bank holidays and school holidays, during evenings in the town centre or police operations the hours are increased to 50 hours per week. The Property Services team will work with the volunteer to analyse demand.

- 3.2 The CCTV supervisor works very closely with the local policing team and can on occasions be called out when an operation is planned and when a particularly serious crime has occurred in the area and where CCTV can play an important part in identifying suspect individuals or vehicles that has been in the town centre on that evening.
- 3.3 In order to support the police the CCTV supervisor will change or increase his hours to help with any police operations. Recent operations have included targeting public order offences, anti-social behaviour (ASB), assault, violent attacks involving hand held weapons/chemicals, drug related offences and shop lifting. This time is re-charged accordingly to the Police, which is time and date dependent upon receipt of the request.
- 3.4 It was identified that some of the tall trees and bushes in the town centre, around the multi-story car park and the Market car park are impeding the vision of the cameras. Work has been completed to reduce the branches and foliage in order to allow for better views and tracking of individuals, vehicles or activity.
- 3.5 As part of the operational review we intend to ensure that the CCTV operator receives payment for services where applicable. We will as well establish where the boundary for voluntary work starts and finishes. The CCTV operator has recently won two separate awards in recognition of contribution to policing in Devon.

4.0 **Incidents**

- 4.1 In the last 12 months the police have made 65 formal requests and daily live requests which are not captured under the formal system for CCTV footage in relation to incidents that have occurred in the Town Centre area. Time is also spent searching for any useful evidence relating to criminal activity or vehicles that can assist police investigations. Gaining intelligence regarding the movement of known individuals and their associates' helps give the police a good overview of their activities and can assist when planning warrants or operations.
- 4.2 During this reporting period there have been authorised requests from the CCTV operator relating to a traffic incident for insurance purposes, a number of serious assaults, some including weapons, a rape, and a missing person incident, that was captured on the cameras.
- 4.3 Regular phone calls are received by members of the community asking for footage relating to damage to their vehicles but these are then routed via the Police and their insurance company. The CCTV operator will review the information required and will release CCTV images in accordance with data protection requirements.

4.4 It is not easy to identify how many cases go to court where CCTV footage has been requested by the police as it is not always possible to get the information from the CPS or the courts. However if the CCTV Operator has witnessed any incidents in 'live view' he will provide a statement to the police at the same time as providing the footage. In these cases we may get notification of the case results directly from the court.

5.0 Stakeholders

5.1 Mid Devon continues to liaise with other agencies that have an interest in the town CCTV system. This includes the police, Town Council and local traders.

5.2 At the Environmental Policy Group meeting on Tuesday 6 August 2019 the Group Manager for Corporate Property and Commercial Assets received a public question regarding mobile CCTV units following reports of Anti-Social Behaviour and littering at the West Exe Recreational ground. The costs of providing mobile CCTV units would be circa £4k for one unit. There would be an ongoing cost of circa £1.8k per annum for 4G air time. There is an option for a free trial. There is no budget planned for mobile CCTV units in the 2020/21 budget.

6.0 Financial

6.1 The operation budget for the Tiverton Town Centre CCTV system in the 2019/20 financial year is £8,310 with an annual contribution from Tiverton Town Council of £6k.

7.0 Conclusion

7.1 The cameras in the town are proving their worth against crime and identifying local criminal activity, however this has been on the increase and a number of traders are concerned about crime prevention particularly in Gold Street, Tiverton.

7.2 The Property Services team will conduct an assessment to ensure that the Council is operating its CCTV system in accordance with the latest Information Commissioners Office (ICO) guidance and to update existing procedures to determine how the CCTV system is used in practice

7.3 The Council will be liaising with Police Representatives to review procedures on time allocation for when the services of the CCTV operator is required.

7.4 The Property Services team will also investigate if our CCTV systems could assist with environmental enforcement investigations such as fly tipping.

Contact for more Information: Andrew Busby, Group Manager for Corporate Property and Commercial Assets. Email: abusby@middevon.gov.uk Telephone: 01884 234948

Circulation of the Report: Cllr Simon Clist, Leadership Team.

List of Background Papers: None.

Guidelines



EDPB Plenary meeting, 09-10 July 2019

Guidelines 3/2019 on processing of personal data through video devices

Version for public consultation

Adopted on 10 July 2019

Table of contents

1	Introduction.....	4
2	Scope of application	5
2.1	Personal Data	5
2.2	Application of the Law Enforcement Directive, LED (EU2016/680).....	5
2.3	Household exemption	6
3	Lawfulness of processing.....	7
3.1	Legitimate interest, Article 6 (1) (f)	7
3.1.1	Existence of legitimate interests	8
3.1.2	Necessity of processing	8
3.1.3	Balancing of interests	9
3.2	Necessity to perform a task carried out in the public interest or in the exercise of official authority vested in the controller, Article 6 (1) (e)	11
3.3	Consent, Article 6 (1) (a).....	12
4	Disclosure of video footage to third parties.....	12
4.1	Disclosure of video footage to third parties in general.....	12
4.2	Disclosure of video footage to law enforcement agencies	13
5	Processing of special categories of data	14
5.1	General considerations when processing biometric data.....	15
5.2	Suggested measures to minimize the risks when processing biometric data	18
6	Rights of the data subject.....	18
6.1	Right to access.....	18
6.2	Right to erasure and right to object	20
6.2.1	Right to erasure (Right to be forgotten).....	20
6.2.2	Right to object	20
7	Transparency and information obligations	21
7.1	First layer information (warning sign)	22
7.1.1	Positioning of the warning sign	22
7.1.2	Content of the first layer	22
7.2	Second layer information	23
8	Storage periods and obligation to erasure.....	24
9	Technical and organisational measures	24
9.1	Overview of video surveillance system	25
9.2	Data protection by design and by default.....	26
9.3	Concrete examples of relevant measures.....	26

9.3.1	Organisational measures.....	27
9.3.2	Technical measures	28
10	Data protection impact assessment.....	28

The European Data Protection Board

Having regard to Article 70 (1e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 12 and Article 22 of its Rules of Procedure of 25 May 2018, revised on 23 November 2018,

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. The intensive use of video devices has an impact on citizen’s behaviour. Significant implementation of such tools in many spheres of the individuals’ life will put an additional pressure on the individual to prevent the detection of what might be perceived as anomalies. De facto, these technologies may limit the possibilities of anonymous movement and anonymous use of services and generally limit the possibility of remaining unnoticed. Data protection implications are massive.
2. While individuals might be comfortable with video surveillance set up for a certain security purpose for example, guarantees must be taken to avoid any misuse for totally different and – to the data subject – unexpected purposes (e.g. marketing purpose, employee performance monitoring etc.). In addition, many tools are now implemented to exploit the images captured and turn traditional cameras into smart cameras. The amount of data generated by the video, combined with these tools and techniques increase the risks of secondary use (whether related or not to the purpose originally assigned to the system) or even the risks of misuse. The general principles in GDPR (Article 5), should always be carefully considered when dealing with video surveillance.
3. Video surveillance systems in many ways change the way professionals from the private and public sector interact in private or public places for the purpose of enhancing security, obtaining audience analysis, delivering personalized advertising, etc. Video surveillance has become high performing through the growing implementation of intelligent video analysis. These techniques can be more intrusive (e.g. complex biometric technologies) or less intrusive (e.g. simple counting algorithms). Remaining anonymous and preserving one’s privacy is in general increasingly difficult. The data protection issues raised in each situation may differ, so will the legal analysis when using one or the other of these technologies.
4. In addition to privacy issues, there are also risks related to possible malfunctions of these devices and the biases they may induce. Researchers report that software used for facial identification, recognition, or analysis performs differently based on the age, gender, and ethnicity of the person it’s identifying. Algorithms would perform based on different demographics, thus, bias in facial recognition threatens to reinforce the prejudices of society. That is why, data controllers must also ensure that biometric

data processing deriving from video surveillance be subject to regular assessment of its relevance and sufficiency of guarantees provided.

5. Video surveillance is not by default a necessity when there are other means to achieve the underlying purpose. Otherwise we risk a change in cultural norms leading to the acceptance of lack of privacy as the general outset.
6. These guidelines aim at giving guidance on how to apply the GDPR in relation to processing personal data through video devices. The examples are not exhaustive, the general reasoning can be applied to all potential areas of use.

2 SCOPE OF APPLICATION¹

2.1 Personal Data

7. Systematic automated monitoring of a specific space by optical or audio-visual means, mostly for property protection purposes, or to protect individual's life and health, has become a significant phenomenon of our days. This activity brings about collection and retention of pictorial or audio-visual information on all persons entering the monitored space that are identifiable on basis of their looks or other specific elements. Identity of these persons may be established on grounds of these details. It also enables further processing of personal data as to the persons' presence and behaviour in the given space. The potential risk of misuse of these data grows in relation to the dimension of the monitored space as well as to the number of persons frequenting the space. This fact is reflected by the General Data Protection Regulation in the Article 35 (3) (c) which requires the carrying out of a data protection impact assessment in case of a systematic monitoring of a publicly accessible area on a large scale, as well as in Article 37 (1) (b) which requires processors to designate a data protection officer, if the processing operation by its nature entails regular and systematic monitoring of data subjects.
8. However, the Regulation does not apply to processing of data that has no reference to a person, e.g. if an individual cannot be identified, directly or indirectly.

Example: The GDPR is not applicable for fake cameras (i.e. any camera that is not functioning as a camera and thereby is not processing any personal data). *However, in some Member States it might be subject to other legislation.*

Example: Recordings from a high altitude only fall under the scope of the GDPR if under the circumstances the data processed can be related to a specific person.

Example: A video camera is integrated in a car for providing parking assistance. If the camera is constructed or adjusted in such a way that it does not collect any information relating to a natural person (such as licence plates or information which could identify passers-by) the GDPR does not apply.

- 9.
10. Notably processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,

¹ The EDPB notes that where the GDPR so allows, specific requirements in national legislation might apply.

including the safeguarding against and the prevention of threats to public security, falls under the directive EU2016/680.

2.3 Household exemption

11. Pursuant to Article 2 (2) (c), the processing of personal data by a natural person in the course of a purely personal or household activity, which can also include online activity, is out of the scope of the GDPR.²
12. This provision – the so-called household exemption – in the context of video surveillance must be narrowly construed. Hence, as considered by the European Court of Justice, the so called “household exemption” must “*be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people*”.³ Furthermore, if a video surveillance system, to the extent it involves the constant recording and storage of personal data and covers, “*even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely ‘personal or household’ activity for the purposes of the second indent of Article 3(2) of Directive 95/46*”⁴.
13. What regards video devices operated inside a private person’s premises, it may fall under the household exemption. It will depend on several factors, which all have to be considered in order to reach a conclusion. Besides the above mentioned elements identified by ECJ rulings, the user of video surveillance at home needs to look at whether he has some kind of personal relationship with the data subject, whether the scale or frequency of the surveillance suggests some kind of professional activity on his side, and of the surveillance’s potential adverse impact on the data subjects. The presence of any single one of the aforementioned elements does not necessarily suggest that the processing is outside the scope of the household exemption, an overall assessment is needed for that determination.

² See also Recital 18.

³ European Court of Justice, Judgment in Case C-101/01, *Bodil Lindqvist case*, 6th November 2003, para 47.

⁴ European Court of Justice, Judgment in Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, 11 December 2014, para. 33.

Example: A tourist is recording videos both through his mobile phone and through a camcorder to document his holidays. He shows the footage to friends and family but does not make it accessible for an indefinite number of people. This would fall under the household exemption.

Example: A downhill mountainbiker wants to record her descent with an actioncam. She is riding in a remote area and only plans to use the recordings for her personal entertainment at home. This would fall under the household exemption.

Example: Somebody is monitoring and recording his own garden. The property is fenced and only the controller himself and his family are entering the garden on a regular basis. This would fall under the household exemption, provided that the video surveillance does not extend even partially to a public space or neighbouring property.

14.

3 LAWFULNESS OF PROCESSING

15. Before use, the purposes of processing have to be specified in detail (Article 5 (1) (b)). Video surveillance can serve many purposes, e.g. protection of property and other assets, collecting evidence for civil claims.⁵ These monitoring purposes should be documented in writing (Article 5 (2)) and need to be specified for every surveillance camera in use. Cameras that are used for the same purpose by a single controller can be documented together, as long as every camera in use has a documented purpose. Furthermore, data subjects must be informed of the purpose(s) of the processing in accordance with Article 13 (*see section 7, Transparency and information obligations*). Video surveillance based on the mere purpose of “safety” or “for your safety” is not sufficiently specific (Article 5 (1) (b)). It is furthermore contrary to the principle that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (see Article 5 (1) (a)).
16. In principle, every legal ground under Article 6 (1) can provide a legal basis for processing video surveillance data. For example, Article 6 (1) (c) applies, where national law stipulates an obligation to video surveillance.⁶ However in practice, the provisions most likely to be used are
-) Article 6 (1) (f) (legitimate interest).
 -) Article 6 (1) (e) (necessity to perform a task carried out in the public interest or in the exercise of official authority)

In rather exceptional cases Article 6 (1) (a) (consent) might be used as a legal basis by the controller.

3.1 Legitimate interest, Article 6 (1) (f)

17. The legal assessment of Article 6 (1) (f) should be based on the following criteria in compliance with Recital 47.

5 Rules on collecting evidence for civil claims varies in member states.

6 These guidelines do not analyse or go into details of national law that might differ between member states.

3.1.1 Existence of legitimate interests

18. Video surveillance is lawful if it is necessary in order to meet the purpose of a legitimate interest pursued by a controller or a third party, unless such interests are overridden by the data subject's interests or fundamental rights and freedoms (Article 6 (1) (f)). Legitimate interests pursued by a controller or a third party can be legal,⁷ economic or non-material interests.⁸ However, the controller should consider that if a the data subject objects to the surveillance in accordance with Article 21 the controller can only proceed with the video surveillance of that data subject if it is a *compelling* legitimate interest which overrides the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
19. Given a real and hazardous situation, the purpose to protect property against burglary, theft or vandalism can constitute a legitimate interest for video surveillance.
20. The legitimate interest needs to be of real existence and has to be a present issue (i.e. it must not be fictional or speculative)⁹. A real-life situation of distress needs to be at hand – such as damages or serious incidents in the past – before starting the surveillance. In light of the principle of accountability, controllers would be well advised to document relevant incidents (date, manner, financial loss) and related criminal charges. Those documented incidents can be a strong evidence for the existence of a legitimate interest.

Example: A shop owner wants to open a new shop and wants to install a video surveillance system. He can show, by presenting statistics, that there is a high expectation of vandalism in the near neighbourhood. Also, experience from neighbouring shops is useful. It is not necessary that a damage to the controller in question must have occurred. It is however not sufficient to present national or general crime statistic without analysing the area in question or the dangers for this specific shop.

- 21.
22. Imminent danger situations may constitute a legitimate interest, such as shops selling precious goods (e.g. jewellers), or areas that are known to be typical crime scenes for property offences (e. g. petrol stations).
23. The GDPR also clearly states that public authorities cannot rely their processing on the grounds of legitimate interest, as long as they are carrying out their tasks, Article 6 (1) sentence 2.

3.1.2 Necessity of processing

24. Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'), see Article 5 (1) (c). Before installing a video-surveillance system the controller should always critically examine if this measure is firstly suitable to attain the desired goal, and secondly adequate and necessary for its purposes. Video surveillance measures should only be chosen if the purpose of the processing could not reasonably be fulfilled by other means which are less intrusive to the fundamental rights and freedoms of the data subject.
25. Given the situation that a controller wants to prevent property related crimes, instead of installing a video surveillance system the controller could also take alternative security measures such as fencing the property, installing regular patrols of security personnel, using gatekeepers, providing better

7 European Court of Justice, Judgment in Case C-13/16, *Rīgas satiksme case*, 4 may 2017

8 see wp 217, Article 29 Working Party.

9 see wp 217, Article 29 Working Party, p. 24 seq.

lighting, installing security locks, tamper-proof windows and doors or applying anti-graffiti coating or foils to walls. Those measures can be as effective as video surveillance systems against burglary, theft and vandalism.

26. Before operating a camera system, the controller is obliged to assess where and when video surveillance measures are strictly necessary. Usually a surveillance system operating at night-time as well as outside the regular working hours will meet the needs of the controller to prevent any dangers to his property.
27. In general, the necessity to use video surveillance to protect the controllers' premises ends at the property boundaries.¹⁰ However, there are cases where the surveillance of the property is not sufficient for an effective protection. In some individual cases it might be necessary to exceed the video surveillance to the immediate surroundings of the premises. In this context, the controller should consider physical and technical means, for example blocking out or pixelating not relevant areas.

Example: A bookshop wants to protect its premises against vandalism. In general, cameras should only be filming the premises itself because it is not necessary to watch neighbouring premises or public areas in the surrounding of the bookshop premises for that purpose.

- 28.
29. Questions concerning the processing's necessity also arise regarding the way evidence is preserved. In some cases it might be necessary to use black box solutions where the footage is automatically deleted after a certain storage period and only accessed in case of an incident. In other situations it might not be necessary to record the video material at all but more appropriate to use real-time monitoring instead. The decision between black box solutions and real-time monitoring should also be based on the purpose pursued. If for example the purpose of video surveillance is the preservation of evidence, real-time methods are usually not suitable. Sometimes real-time monitoring may also be more intrusive than storing and automatically deleting material after a limited timeframe. The data minimisation principle must be regarded in this context (Article 5 (1) (c)). It should also be kept in mind that it might be possible that the controller could use security personnel instead of video surveillance that are able to react and intervene immediately.

3.1.3 Balancing of interests

30. Presuming that video surveillance is necessary to protect the legitimate interests of a controller, a video surveillance system may only be put in operation, if the legitimate interests of the controller or those of a third party (e.g. protection of property or physical integrity) are not overridden by the interests or fundamental rights and freedoms of the data subject. The controller needs to consider 1) to what extent the monitoring affects legitimate interests, fundamental rights, and freedoms of individuals and 2) if this causes violations or negative consequences with regard to the data subject's rights. In fact, balancing the interests is mandatory. Fundamental rights and freedoms on one hand and the controller's legitimate interests on the other hand have to be evaluated and balanced carefully.

¹⁰ This might also be subject to national legislation in some member states.

Example: A private parking company has documented reoccurring problems with thefts in the cars parked. The parking area is an open space and can be easily accessed by anyone, but is clearly marked with signs and road blockers surrounding the space. The parking company have a legitimate interest (preventing thefts in the customer's cars) to monitor the area during the time of day that they are experiencing problems. Data subjects are monitored in a limited timeframe, they are not in the area for recreational purposes and it is also in their own interest that thefts are prevented. The interest of the data subjects not to be monitored is in this case overridden by the controller's legitimate interest.

Example: A restaurant decides to install video cameras in the restrooms to control the tidiness of the sanitary facilities. In this case the rights of the data subjects clearly overrides the interest of the controller, therefore cameras can't be installed there.

31.

3.1.3.1 *Making case-by-case decisions*

32. As the balancing of interests is mandatory according to the regulation, the decision has to be made on a case-by-case basis (see Article 6 (1) (f)). Referencing abstract situations or comparing similar cases to one another is insufficient. The controller has to evaluate the risks of the intrusion of the data subject's rights; here the decisive criterion is the intensity of intervention for the rights and freedoms of the individual.

33. Intensity can inter alia be defined by the type of information that is gathered (information content), the scope (information density, spatial and geographical extent), the number of data subjects concerned, either as a specific number or as a proportion of the relevant population, the situation in question, the actual interests of the group of data subjects, alternative means, as well as by the nature and scope of the data assessment.

34. Important balancing factors can be the size of the area, which is under surveillance and the amount of data subjects under surveillance. The use of video surveillance in a remote area (e. g. to watch wildlife or to protect critical infrastructure such as a privately owned radio antenna) has to be assessed differently than video surveillance in a pedestrian zone or a shopping mall.

Example: If a dash cam is installed (e. g. for the purpose of collecting evidence in case of an accident), it is important to ensure that this camera is not constantly recording traffic, as well as persons who are near a road. Otherwise the interest in having video recordings as evidence in the more theoretical case of a road accident cannot justify this serious interference with data subject's rights.¹¹

11

3.1.3.2 *Data subjects' reasonable expectations*

35. According to Recital 47, the existence of a legitimate interest needs careful assessment. Here the reasonable expectations of the data subject at the time and in the context of the processing of its personal data have to be included. Concerning systematic monitoring, the relationship between data subject and controller may vary significantly and may affect what reasonable expectations the data subject might have. The interpretation of the concept of reasonable expectations should not only be

11 Even if under some circumstances it might theoretically be possible to identify a legal basis for parts of such surveillance, the controller will still have to comply with the general principles (Art. 5 GDPR) and the transparency obligations to properly inform the data subject (Art. 13 GDPR).

based on the subjective expectations in question. Rather, the decisive criterion has to be if an objective third party could reasonably expect and conclude to be subject to monitoring in this specific situation.

36. For instance, an employee in his/her workplace is in most cases not likely expecting to be monitored by his or her employer.¹² Furthermore, monitoring is not to be expected in one's private garden, in living areas, or in examination and treatment rooms. In the same vein, it is not reasonable to expect monitoring in sanitary or sauna facilities – monitoring such areas is an intense intrusion into the rights of the data subject. The reasonable expectations of data subjects are that no video surveillance will take place in those areas. On the other hand, the customer of a bank might expect that he/she is monitored inside the bank or by the ATM.
37. Data subjects can also expect to be free of monitoring within public areas especially if those public areas are typically used for recovery, regeneration, and leisure activities as well as in places where individuals stay and/or communicate, such as sitting areas, tables in restaurants, parks, cinemas and fitness facilities. Here the legitimate interests or rights and freedoms of the data subject will often override the controller's legitimate interests.

Example: In toilets data subjects expect not to be monitored. Video surveillance for example to prevent accidents is not proportional.

- 38.
39. Signs informing the subject about the video surveillance have no relevance when determining what a data subject objectively can expect.

3.2 Necessity to perform a task carried out in the public interest or in the exercise of official authority vested in the controller, Article 6 (1) (e)

40. Personal data could be processed through video surveillance under Article 6 (1) (e) if it is necessary to perform a task carried out in the public interest or in in the exercise of official authority.¹³ It may be that the exercise of official authority does not allow for such processing, but other legislative bases such as "health and safety" for the protection of employees, visitors and employees may provide limited scope for processing, while still having regard for GDPR obligations and data subject rights.
41. Member States may maintain or introduce specific national legislation for video surveillance to adapt the application of the rules of the GDPR by determining more precisely specific requirements for processing as long as it is in accordance with the principles laid down by the GDPR (e.g. storage limitation, proportionality).

12 See also: Article 29 Working Party, Opinion 2/2017 on data processing at work, WP249, adopted on 8 June 2017.

13 «The basis for the processing referred shall be laid down by Union law or Member State law» and «shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6 (3)).

3.3 Consent, Article 6 (1) (a)

42. Consent has to be freely given, specific, informed and unambiguous as described in the guidelines on consent.¹⁴
43. Regarding systematic monitoring, the data subject's consent can only serve as a legal basis in accordance with Article 7 (see Recital 43) in exceptional cases. It is in the surveillance's nature that this technology monitors an unknown number of people at once. The controller will hardly be able to prove that the data subject has given consent prior to processing of its personal data (Article 7 (1)). Assumed that the data subject withdraws its consent it will be difficult for the controller to prove that personal data is no longer processed (Article 7 (3)).

Example: Athletes may request monitoring during individual exercises in order to analyse their techniques and performance. On the other hand, where a sports club takes the initiative to monitor a whole team for the same purpose, consent will often not be valid, as the individual athletes may feel pressured into giving consent so that their refusal of consent does not adversely affect teammates.

- 44.
45. If the controller wishes to rely on consent it is his duty to make sure that every data subject who enters the area which is under video surveillance has given her or his consent. This consent has to meet the conditions of Article 7. Entering a marked monitored area (e.g. people are invited to go through a specific hallway or gate to enter a monitored area), does not constitute a statement or a clear affirmative action needed for consent, unless it meets the criteria of Article 4 and 7 as described in the guidelines on consent.¹⁵
46. Given the imbalance of power between employers and employees, in most cases employers should not rely on consent when processing personal data, as it is unlikely to be freely given. The guidelines on consent should be taken into consideration in this context.
47. Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context (see Article 88).

4 DISCLOSURE OF VIDEO FOOTAGE TO THIRD PARTIES

48. In principle, the general regulations of the GDPR apply to the disclosure of video recordings to third parties.

4.1 Disclosure of video footage to third parties in general

49. Disclosure is defined in Article 4 (2) as transmission (e.g. individual communication), dissemination (e.g. publishing online) or otherwise making available. Third parties are defined in Article 4 (10). Where disclosure is made to third countries or international organisations, the special provisions of Article 44 et seq. also apply.

14 In addition, the Article 29 Working Party (Art. 29 WP) adopted „Guidelines on consent under Regulation 2016/679“ (WP 259 rev. 01) which should be taken in account.

15 In addition, the Article 29 Working Party (Art. 29 WP) adopted „Guidelines on consent under Regulation 2016/679“ (WP 259) which should be taken in account.

50. Any disclosure of personal data is a separate kind of processing of personal data for which the controller needs to have a legal basis in Article 6.

Example: A controller who wishes to upload a recording to the Internet needs to rely on a legal basis for that processing, for instance by obtaining consent from the data subject according to Article 6 (1) (a).

- 51.
52. The transmission of video footage to third parties for the purpose other than that for which the data has been collected is possible under the rules of Article 6 (4).

Example: Video surveillance of a barrier (at a parking lot) is installed for the purpose of resolving damages. A damage occurs and the recording is transferred to a lawyer to pursue a case. In this case the purpose for recording is the same as the one for transferring.

Example: Video surveillance of a barrier (at a parking lot) is installed for the purpose of resolving damages. The recording is published online for pure amusement reasons. In this case the purpose has changed and is not compatible with the initial purpose. It would furthermore be problematic to identify a legal basis for that processing (publishing).

- 53.
54. A third party recipient will have to make its own legal analysis, in particular identifying its legal basis under Article 6 for his processing (e.g. receiving the material).

4.2 Disclosure of video footage to law enforcement agencies

55. The disclosure of video recordings to law enforcement agencies is also an independent process, which requires a separate justification for the controller.
56. According to Article 6 (1) (c), processing is legal if it is necessary for compliance with a legal obligation to which the controller is subject. Although the applicable police law is an affair under the sole control of the member states, there are most likely general rules that regulate the transfer of evidence to law enforcement agencies in every member state. The processing of the controller handing over the data is regulated by the GDPR. If national legislation requires the controller to cooperate with law enforcement (e. g. investigation), the legal basis for handing over the data is legal obligation under Article 6 (1) (c).
57. The purpose limitation in Article 6 (4) is then often unproblematic, since the disclosure explicitly goes back to member state law. A consideration of the special requirements for a change of purpose in the sense of lit. a - e is therefore not necessary.

Example: A shop owner records footage at its entrance. It records a person stealing another person's wallet. The police asks the controller to hand over the material in order to assist in their investigation. In that case the shop owner would use the legal basis under Article 6 (1) (c) (legal obligation) read in conjunction with the relevant national law for the transfer processing.

Example: A camera is installed in a shop for security reasons. The shop owner believes he has recorded something suspicious in his footage and decides to send the material to the police (without any indication that there is an ongoing investigation of some kind). In this case the shop owner has to assess whether the conditions under, in most cases, Article 6 (1) (f) are met.

- 58.

59. The processing of the personal data by the law enforcement agencies themselves does not follow the GDPR (see Article 2 (2) (d)), but follows instead the Law Enforcement Directive (EU2016/680).

5 PROCESSING OF SPECIAL CATEGORIES OF DATA

60. Video surveillance systems usually collect massive amounts of personal data which may reveal data of a highly personal nature and even special categories of data. Indeed, apparently non-significant data originally collected through video can be used to infer other information to achieve a different purpose (e.g. to map an individual's habits). However, video surveillance is not always considered to be processing of special categories of personal data.

Example: Video footage showing a data subject wearing glasses or using a wheel chair are not per se considered to be special categories of personal data.

- 61.
62. However, if the video footage is processed to deduce special categories of data Article 9 applies.

Example: Political opinions could for example be deduced from images showing identifiable data subjects taking part in an event, engaging in a strike, etc. This would fall under Article 9.

Example: A hospital installing a video camera in order to monitor a patient's health condition would be considered as processing of special categories of personal data (Article 9).

- 63.
64. In general, as a principle, whenever installing a video surveillance system careful consideration should be given to the data minimization principle. Hence, even in cases where Article 9 (1) does not apply, the data controller should always try to minimize the risk of capturing footage revealing other sensitive data (beyond Article 9), regardless of the aim.

Example: Video surveillance capturing a church does not per se fall under Article 9. However, the controller has to conduct an especially careful assessment under Article 6 (1) (f) taken into account the nature of the data as well as the risk of capturing other sensitive data (beyond Article 9) when assessing the interests of the data subject.

- 65.
66. If a video surveillance system is used in order to process special categories of data, the data controller must identify both an exception for processing special categories of data under Article 9 (i.e. an exemption from the general rule that one should not process special categories of data) and a legal basis under Article 6.
67. For instance, Article 9 (2) (c) (processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent) could – in theory and exceptionally – be used, but the data controller would have to justify it as an absolute necessity to safeguard the vital interests of a person and prove that this person "*is physically or legally incapable of giving his consent*". In addition, the data controller won't be allowed to use the system for any other reason.

Example: A hospital is monitoring a patient for medical reasons. The data subject was brought by ambulance unconscious to the hospital. In this case Article 9 (2) (c) could apply.

- 68.

69. It is important to note here that every exemption listed in Article 9 is not likely to be usable to justify processing of special categories of data through video surveillance. More specifically, data controllers processing those data in the context of video surveillance cannot rely on Article 9 (2) (e), which allows processing that relates to personal data that are manifestly made public by the data subject. The mere fact of entering into the range of the camera does not imply that the data subject intends to make public special categories of data relating to him or her.
70. Furthermore, processing of special categories of data requires a heightened and continued vigilance to certain obligations; for example high level of security and data protection impact assessment where necessary.

Example: An employer must not use video surveillance recordings showing a demonstration in order to identify strikers.

71.

5.1 General considerations when processing biometric data

72. The use of biometric data and in particular facial recognition entail heightened risks for data subjects' rights. It is crucial that recourse to such technologies takes place with due respect to the principles of lawfulness, necessity, proportionality and data minimisation as set forth in the GDPR. Whereas the use of these technologies can be perceived as particularly effective, controllers should first of all assess the impact on fundamental rights and freedoms and consider less intrusive means to achieve their legitimate purpose of the processing.
73. To qualify as biometric data as defined in the GDPR, processing of raw data, such as the physical, physiological or behavioural characteristics of a natural person, must imply a measurement of this characteristics. Since biometric data is the result of such measurements, the GDPR states in its Article 4.14 that it is "*resulting from specific technical processing relating to the physical, physiological or behavioural characteristics*". The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual.¹⁶
74. In order for it to be considered as processing of special categories of personal data (Article 9) it requires that biometric data is processed "for the purpose of uniquely identifying a natural person".
75. To sum up, in light of Article 4.14 and 9, three criteria must be considered:
- **Nature of data** : data relating to physical, physiological or behavioural characteristics of a natural person,
 - **Means and way of processing** : data "resulting from a specific technical processing",
 - **Purpose of processing:** data must be used for the purpose to uniquely identifying a natural person.
76. The use of video surveillance including biometric recognition functionality installed by private entities for their own purposes (e.g. marketing, statistical, or even security) will, in most cases, require

¹⁶ Recital 51 supports this analysis, stating that "*the processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person*".

explicit consent of all data subjects (Article 9 (2) (a)), however another suitable exception in Article 9 could also be applicable.

Example: To improve its service a private company replaces passenger identification check points within an airport (luggage drop-off, boarding) with video surveillance systems that use facial recognition techniques to verify the identity of the passengers that have chosen to consent to such a procedure. Since the processing falls under Article 9, the passengers, who will have previously given their explicit and informed consent, will have to enlist themselves at for example an automatic terminal in order to create and register their facial template associated with their boarding pass and identity. The check points with facial recognition need to be clearly separated, e. g. the system must be installed within a gantry so that the biometric templates of non-consenting person will not be captured. Only the passengers, who will have previously given their consent and proceeded with their enrolment, will use the gantry equipped with the biometric system.

Example: A controller manages access to his building using a facial recognition method. People can only use this way of access if they have given there explicitly informed consent (according to Article 9 (2) (a)) beforehand. However, in order to ensure that no one who has not previously given his or her consent is captured, the facial recognition method should be triggered by the data subject himself, for instance by pushing a button. To ensure the lawfulness of the processing, the controller must always offer an alternative way to access the building, without biometric processing, such as badges or keys.

77.

78. In this type of cases, where biometric templates are generated, controllers shall ensure that once a match or no-match result has been obtained, all the intermediate templates made on the fly (with the explicit and informed consent of the data subject) in order to be compared to the ones created by the data subjects at the time of the enlistment, are immediately and securely deleted. The templates created for the enlistment should only be retained for the realisation of the purpose of the processing and should not be stored or archived.

79. However, when the purpose of the processing is for example to distinguish one category of people from another but not to uniquely identify anyone the processing does not fall under Article 9.

Example: A shop owner would like to customize its advertisement based on gender and age characteristics of the customer captured by a video surveillance system. If that system does not generate biometric templates in order to uniquely identify persons but instead just detects those physical characteristics and consequently only classifies the person, then the processing would not fall under Article 9.

80.

81. However, Article 9 applies if the controller stores biometric data (most commonly through templates that are created by the extraction of key features from the raw form of biometric data (e.g. facial measurements from an image)) in order to uniquely identify a person. If a controller wishes to detect a data subject re-entering the area or entering another area (for example in order to project continued customized advertisement), the purpose would then be to uniquely identify a natural person, meaning that the operation would from the start fall under Article 9. This could be the case if a controller stores generated templates to provide further tailored advertisement on several billboards throughout different locations inside the shop. Since the system is using physical characteristics to detect specific individuals coming back in the range of the camera (like the visitors of a shopping mall) and tracking

them, it would constitute a biometric identification method because it is aimed at recognition through the use of specific technical processing.

Example: A shop owner has installed facial recognition system inside his shop in order to customize its advertisement towards individuals. The data controller has to obtain the explicit and informed consent of all data subjects before using this biometric system and delivering tailored advertisement. The system would be unlawful if it captures visitors or passer-by who have not consented to the creation of their biometric template, even if their template is deleted within the shortest possible period. Indeed, these temporary templates constitute biometric data processed in order to uniquely identify a person who may not want to receive targeted advertisement.

82.

83. The EDPB observes that some biometric systems are installed in uncontrolled environment¹⁷, which means that the system involves capturing on the fly the faces of any individual passing in the range of the camera, including persons who have not consented to the biometric device, and thereby creating biometric templates. These templates are compared to the ones created of data subjects having given their prior consent during an enlistment process (i.e. a biometric device user) in order for the data controller to recognise whether the person is a biometric device user or not. In this case, the system is often designed to discriminate the individuals it wants to recognize from a database from those who are not enlisted. Since the purpose is to uniquely identify natural persons, an exception under Article 9 (2) GDPR is still needed for anyone captured by the camera.

Example: A hotel uses video surveillance to automatically alert the hotel manager that a VIP has arrived when the face of the guest is recognized. These VIPs have priory given their explicit consent to the use of facial recognition before being recorded in a database established for that purpose. These processing systems of biometric data would be unlawful unless all other guests monitored (in order to identify the VIPs) have consented to the processing according to Article 9 (2) (a) GDPR.

Example: A controller installs a video surveillance system with facial recognition at the entrance of the concert hall he manages. The controller must set up clearly separated entrances; one with a biometric system and one without (where you instead for example scan a ticket). The entrances equipped with biometric devices, must be installed and made accessible in a way that prevents the system from capturing biometric templates of non-consenting spectators.

84.

85. Finally, when the consent is required by Article 9 GDPR, the data controller shall not condition the access to its services to the acceptance of the biometric processing. In other words and notably when the biometric processing is used for authentication purpose, the data controller must offer an alternative solution that does not involve biometric processing – without restraints or additional cost for the data subject. This alternative solution is also needed for persons who do not meet the constraints of the biometric device (enrolment or reading of the biometric data impossible, disability situation making it difficult to use, etc.) and in anticipation of unavailability of the biometric device

¹⁷ It means that the biometric device is located in a space open to the public and is able to work on anyone passing by, as opposed to the biometric systems in controlled environments that can be used only by consenting person's participation.

(such as a malfunction of the device), a "back-up solution" must be implemented to ensure continuity of the proposed service, limited however to exceptional use.

5.2 Suggested measures to minimize the risks when processing biometric data

86. In compliance with the data minimization principle, data controllers must ensure that data extracted from a digital image to build a template will not be excessive and will only contain the information required for the specified purpose, thereby avoiding any possible further processing. Measures should be put in place to guarantee that templates cannot be transferred across biometric systems.
87. Identification and authentication/verification are likely to require the storage of the template for use in a later comparison. The data controller must consider the most appropriate location for storage of the data. In an environment under control (delimited hallways or checkpoints), templates shall be stored on an individual device kept by the user and under his or her sole control (in a smartphone or the id card) or - when needed for specific purposes and in presence of objective needs - stored in a centralized database in an encrypted form with a key/secret solely in the hands of the person to prevent unauthorised access to the template or storage location. If the data controller cannot avoid having access to the templates, he must take appropriate steps to ensure the security of the data stored. This may include encrypting the template using a cryptographic algorithm.
88. In any case, the controller shall take all necessary precautions to preserve the availability, integrity and confidentiality of the data processed. To this end, the controller shall notably take the following measures: compartmentalize data during transmission and storage, store biometric templates and raw data or identity data on distinct databases, encrypt biometric data, notably biometric templates, and define a policy for encryption and key management, integrate an organisational and technical measure for fraud detection, associate an integrity code with the data (for example signature or hash) and prohibit any external access to the biometric data.
89. Besides, data controllers shall proceed to the deletion of raw data (face images, speech signals, the gait, etc.) and ensure the effectiveness of this deletion. Indeed, insofar as biometric templates derives from such data, one can consider that the constitution of databases could represent an equal if not even bigger threat (because it may not always be easy to read a biometric template without the knowledge on how it was programmed, whereas raw data will be the building block of any template). In case the data controller would need to keep such data, noise-additive method (such as watermarking) must be explored, which would render the creation of the template ineffective. The controller must also delete biometric data and templates in the event of unauthorized access to the read-comparison terminal or storage server and delete any data not useful for further processing at the end of the biometric device's life.

6 RIGHTS OF THE DATA SUBJECT

90. Due to the character of data processing when using video surveillance some data subject's rights under GDPR serves further clarification. This chapter is however not exhaustive, all rights under the GDPR applies to processing of personal data through video surveillance.

6.1 Right to access

91. A data subject has the right to obtain confirmation from the controller as to whether or not their personal data are being processed. For video surveillance this means that if no data is stored or transferred in any way then once the real-time monitoring moment has passed the controller could only give the information that no personal data is any longer being processed (besides the general

information obligations under Article 13, see *section 7 – Transparency and information obligations*). If however data is still being processed at the time of the request (i.e. if the data is stored or continuously processed in any other way), the data subject should receive access and information in accordance with Article 15.

92. There are however, a number of limitations that may in some cases apply in relation to the right to access.

) Article 15 (4) GDPR, adversely affect the rights of others

93. Given that, any number of data subjects may be recorded in the same sequence of video surveillance a screening would then cause additional processing of personal data of other data subjects. If the data subject wishes to receive a copy of the material (article 15 (3)), this could adversely affect the rights and freedoms of other data subject in the material. To prevent that effect the controller should therefore take into consideration that due to the intrusive nature of the video footage the controller should not in some cases hand out video footage where other data subjects can be identified. The protection of the rights of third parties should however not be used as an excuse to prevent legitimate claims of access by individuals, the controller should instead implement technical measures to fulfil the access request (for example, image-editing such as masking or scrambling).

) Article 11 (2) GDPR, controller is unable to identify the data subject

94. If the video footage is not searchable for personal data, (i.e. the controller would likely have to go through a large amount of stored material in order to find the data subject in question) the controller may be unable to identify the data subject.
95. For these reasons the data subject should (besides identifying themselves including with identification document or in person) in its request to the controller, specify when – within a reasonable timeframe in proportion to the amount of data subjects recorded – he or she entered the monitored area. The controller should notify the data subject beforehand on what information is needed in order for the controller to comply with the request. If the controller is able to demonstrate that it is not in a position to identify the data subject, the controller must inform the data subject accordingly, if possible.

Example: If a data subject is requesting a copy of his or her personal data processed through video surveillance at the entrance of a shopping mall with 30 000 visitors per day, the data subject should specify when he or she passed the monitored area within approximately a two-hour-timeframe. If the controller still processes the material a copy of the video footage should be provided. If other data subjects can be identified in the same material then that part of the material should be anonymised (for example by blurring the copy or parts thereof) before giving the copy to the data subject that filed the request.

Example: If the controller is automatically erasing all footage for example within 2 days, a data subject may only get access to that very information [that the material has been deleted] if the request is presented to the controller post those 2 days.

- 96.

) Article 12 GDPR, excessive requests

97. In case of excessive or manifestly unfounded requests from a data subject, the controller may either charge a reasonable fee in accordance with Article 12 (5) (a) GDPR, or refuse to act on the request (Article 12 (5) (b) GDPR. The controller needs to be able to demonstrate the excessive or manifestly unfounded character of the request.

6.2 Right to erasure and right to object

6.2.1 Right to erasure (Right to be forgotten)

98. If the controller continues to process personal data beyond real-time monitoring (e.g. storing) the data subject may request for the personal data to be erased under Article 17 GDPR.
99. Upon a request, the controller is obliged to erase the personal data without undue delay if one of the circumstances listed under Article 17 (1) GDPR applies (and none of the exceptions listed under Article 17 (3) GDPR does). That includes the obligation to erase personal data when they are no longer needed for the purpose for which they were initially stored, or when the processing is unlawful (see also section 8 on storage periods and obligation to erasure). Furthermore, depending on the legal basis of processing, personal data should be erased:
- *for consent* whenever the consent is withdrawn (and there is no other legal basis for the processing)
 - for Legitimate interest:
 - o whenever the data subject exercises the right to object (see *section 6.2.2*) and there are no overriding compelling legitimate grounds for the processing, or
 - o in case of direct marketing (including profiling) whenever the data subject objects to the processing.
100. If the controller has made the video footage public (e.g. broadcasting or streaming online), reasonable steps need to be taken in order to inform other controllers (that are now processing the personal data in question) of the request pursuant to Article 17 (2) GDPR. The reasonable steps should include technical measures, taking into account available technology and the cost of implementation. To the extent possible, the controller should notify – upon erasure of personal data – anyone to which the personal data previously have been disclosed, in accordance with Article 19 GDPR.
101. Besides the controller’s obligation to erase personal data upon the data subject’s request, the controller is obliged under the general principles of the GDPR to limit the personal data stored (see *section 8*).
102. For video surveillance it is worth noticing that by for instance blurring the picture with no retroactive ability to recover the personal data the picture previously contained, the personal data are considered erased in accordance with GDPR.

Example: A convenience store is having trouble with vandalism in particular on its exterior and is therefore using video surveillance outside of their entrance in direct connection to the walls. A passer-by requests to have his personal data erased from that very moment. The controller is obliged to respond to the request without undue delay and at the latest within one month. Since the footage in question does no longer meet the purpose for which it was initially stored (no vandalism occurred during the time the data subject passed by), there is at the time of the request, no legitimate interest to store the data that would override the interests of the data subjects. The controller needs to erase the personal data.

103.

6.2.2 Right to object

104. For video surveillance based on *legitimate interest* (Article 6 (1) (f) GDPR) or for the necessity when carrying out a task in the *public interest* (Article 6 (1) (e) GDPR) the data subject has the right – at any time – to object, on grounds relating to his or her particular situation, to the processing in accordance

with Article 21 GDPR. Unless the controller demonstrates compelling legitimate grounds that overrides the rights and interests of the data subject, the processing of data of the individual who objected must then stop. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month.

105. In the context of video surveillance this objection could be made either prior to entering, during the time in, or after leaving, the monitored area. In practice this means that unless the controller has compelling legitimate grounds, monitoring an area where natural persons could be identified is only lawful if either
- (1) the controller is able to immediately stop the camera from processing personal data when requested, or
 - (2) the monitored area is in such detail restricted so that the controller can assure the approval from the data subject prior to entering the area and it is not an area that the data subject as a citizen is entitled to access.
106. When using video surveillance for direct marketing purposes, the data subject has the right to object to the processing on a discretionary basis as the right to object is absolute in that context (Article 21 (2) and (3) GDPR).

Example: A company is experiencing difficulties with security breaches in their public entrance and is using video surveillance on the grounds of legitimate interest, with the purpose to catch those unlawfully entering. A visitor objects to the processing of his or her data through the video surveillance system on grounds relating to his or her particular situation. The company however in this case rejects the request with the explanation that the footage stored is needed due to an ongoing internal investigation, thereby having compelling legitimate grounds to continue processing the personal data.

107.

7 TRANSPARENCY AND INFORMATION OBLIGATIONS¹⁸

108. It has long been inherent to European data protection law that data subjects should be aware of the fact that video surveillance is in operation. They should be informed in a detailed manner as to the places monitored.¹⁹ Under the GDPR the general transparency and information obligations are set out in Article 12 GDPR et seqq. Article 29 Working Party's "Guidelines on transparency under Regulation 2016/679 (WP260)" which were endorsed by the EDPB on May 25th 2018 provide further details. In line with WP260 para. 26, it is Article 13 GDPR, which is applicable if personal data are collected "from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras)".
109. In light of the volume of information, which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency (WP260, par. 35; WP89, p. 22). Regarding video surveillance the most important

¹⁸ Specific requirements in national legislation might apply.

¹⁹ Article 29 Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance (WP89).

information should be displayed on the warning sign itself (first layer) while the further mandatory details may be provided by other means (second layer).

7.1 First layer information (warning sign)

110. The first layer concerns the primary way in which the controller first engages with the data subject. At this stage, controllers may use a warning sign showing the relevant information. The displayed information may be provided in combination with an icon in order to give, in an easily visible, intelligible and clearly readable manner, a meaningful overview of the intended processing (Article 12 (7) GDPR). The format of the information should be adjusted to the individual location (WP89 p. 22).

7.1.1 Positioning of the warning sign

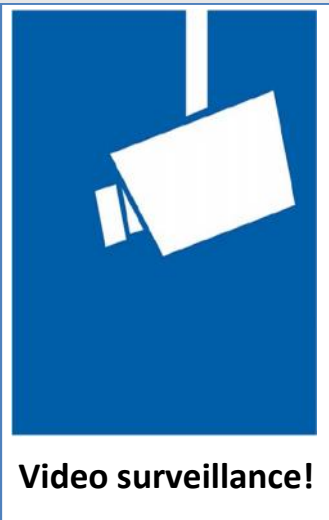
111. The information should be positioned at a reasonable distance from the places monitored (WP 89, p. 22) in such a way that the data subject can easily recognize the circumstances of the surveillance before entering the monitored area (approximately at eye level). It is not necessary to specify the precise location of the surveillance equipment as long as there is no doubt, as to which areas are subject to monitoring and the context of surveillance is to be clarified unambiguously (WP 89, p. 22). The data subject must be able to estimate which area is captured by a camera so that he or she is able to avoid surveillance or adapt his or her behaviour if necessary.

7.1.2 Content of the first layer

112. The first layer information (warning sign) should generally convey the most important information, e.g. the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impacts of the processing.²⁰ This can include for example the legitimate interests pursued by the controller (or by a third party) and contact details of the data protection officer (if applicable). It also has to refer to the more detailed second layer of information and where and how to find it.
113. In addition the sign should also contain any information that could surprise the data subject (WP260, par. 38). That could for example be transmissions to third parties, particularly if they are located outside the EU, and the storage period. If this information is not indicated, the data subject should be able to trust that there is solely a live monitoring (without any data recording or transmission to third parties).

20 See WP260, par. 38

Example:



Further information is available:
J via notice
J at our reception/ customer
information/ register
J via internet (URL)...

Identity of the controller and, where applicable, of the controller's representative:

Contact details of the data protection officer (where applicable):

Purposes of the processing for which the personal data are intended as well as the legal basis for the processing:

Data subjects rights: As a data subject you have several rights against the controller, in particular the right to request from the controller access to or erasure of your personal data.

For details on this video surveillance including your rights, see the full information provided by the controller through the options presented on the left.

114.

7.2 Second layer information

115. The second layer information must also be made available at a place easily accessible to the data subject, for example as a complete information sheet available at a central location (e.g. information desk, reception or cashier) or displayed on an easy accessible poster. As mentioned above, the first layer warning sign has to refer clearly to the second layer information. In addition, it is best if the first layer information refers to a digital source (e.g. QR-code or a website address) of the second layer. However, the information should also be easily available non-digitally. In any case, it must be possible to access the second layer information without entering the surveyed area. This can be achieved for example by a link or any other appropriate means like a phone number that can be called. It must contain all other information that is mandatory under Article 13 GDPR.

116. In addition to these options, and also to make them more effective, the EDPB promotes the use of technological means to provide information to data subjects. This may include for instance; geolocating cameras and including information in mapping apps or websites so that individuals can easily, on the one hand, identify and specify the video sources related to the exercise of their rights, and on the other hand, obtain more detailed information on the processing operation.

Example: A shop owner is monitoring his shop. To comply with Article 13 it is sufficient to place a warning sign at an easy visible point at the entrance of his shop, which contains the first layer information. In addition, he has to provide an information sheet containing the second layer information at the cashier or any other central and easy accessible location in his shop.

117.

8 STORAGE PERIODS AND OBLIGATION TO ERASURE

118. Personal data may not be stored longer than what is necessary for the purposes for which the personal data is processed (Article 5 (1) (c) and (e) GDPR). In some member states, there may be specific provisions for storage periods with regards to video surveillance in accordance with Article 6 (2) GDPR.
119. Whether the personal data is necessary to store or not, should be controlled within a narrow timeline. In general, legitimate purposes for video surveillance are often property protection or preservation of evidence. Usually damages that occurred can be recognized within one or two days. Taking into consideration the principles of Article 5 (1) (c) and (e) GDPR, namely data minimization and storage limitation, the personal data should in most cases (e.g. for the purpose of detecting vandalism) be erased, ideally automatically, after a few days. The longer the storage period is set (especially when beyond 72 hours), the more argumentation for the legitimacy of the purpose and the necessity of storage has to be provided. If the controller uses video surveillance not only for monitoring its premises but also intends to store the data, the controller must assure that the storage is actually necessary in order to achieve the purpose. If so, the storage period needs to be clearly defined and individually set for each particular purpose. It is the controller's responsibility to define the retention period in accordance with the principles of necessity and proportionality and to demonstrate compliance with the provisions of the GDPR.

Example: An owner of a small shop would normally take notice of any vandalism the same day. In consequence, a regular storage period of 24 hours is sufficient. Closed weekends or holidays might however be reasons for a longer storage period. If a damage is detected he may also need to store the video footage a longer period in order to take legal action against the offender.

120.

9 TECHNICAL AND ORGANISATIONAL MEASURES

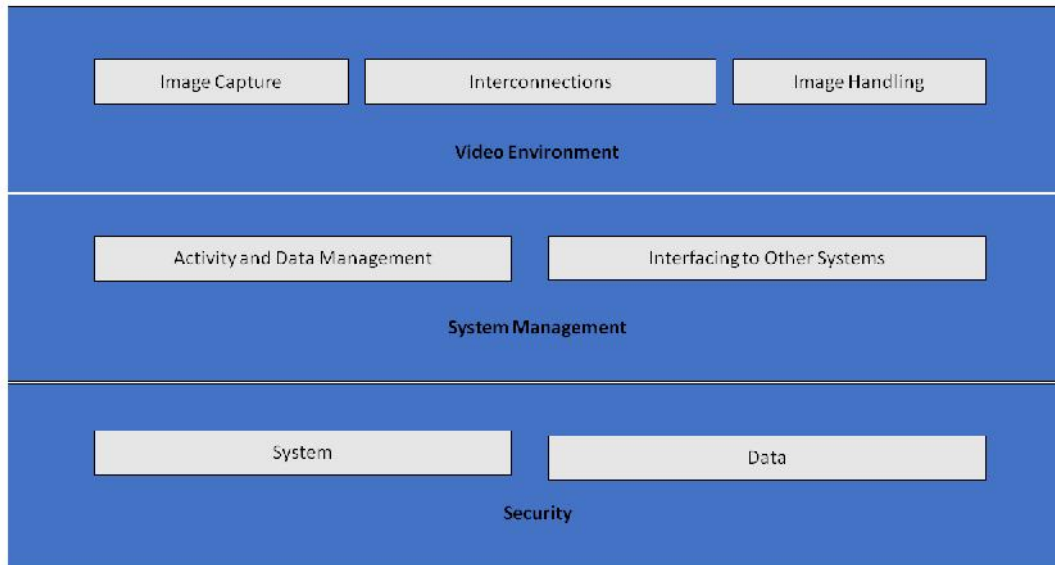
121. As stated in Article 32 (1) GDPR, processing of personal data during video surveillance must not only be legally permissible but controllers and processors must also adequately secure it. Implemented **organizational and technical measures** must be **proportional to the risks to rights and freedoms of natural persons**, resulting from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to video surveillance data. According to Article 24 and 25 GDPR, controllers need to implement technical and organisational measures also in order to safeguard all data-protection principles during processing, and to establish means for data subjects to exercise their rights as defined in Articles 15 – 22 GDPR. Data controllers should adopt internal framework and policies that ensure this implementation both at the time of the determination of the means for processing and at the time of the processing itself, including the performance of data protection impact assessments when needed.

9.1 Overview of video surveillance system

A video surveillance system (VSS)²¹ consists of analogue and digital devices as well software for the purpose of capturing images of a scene, handling the images and displaying them to an operator. Its components are grouped into the following categories:

-) Video environment: image capture, interconnections and image handling
 - the purpose of image capture is generation of an image of the real world in such format that it can be used by the rest of the system
 - interconnections describe all transmission of data within the video environment, i.e. connections and communications. Examples of connections are cables, digital networks, and wireless transmissions. Communications describe all video and control data signals, which could be digital or analogue
 - image handling includes analysis, storage and presentation of an image or a sequence of images
-) From the system management perspective, a VSS has the following logical functions:
 - data management and activity management, which includes handling operator commands and system generated activities (alarm procedures, alerting operators)
 - interfaces to other systems might include connection to other security (access control, fire alarm) and non-security systems (building management systems, automatic license plate recognition)
-) VSS security consists of system and data confidentiality, integrity and availability
 - system security includes physical security of all system components and control of access to the VSS
 - data security includes prevention of loss or manipulation of data

²¹ GDPR does not provide a definition for it, a technical description can for example be found in EN 62676-1-1:2014 Video surveillance systems for use in security applications – Part 1-1: Video system requirements.



122.

Figure 1- video surveillance system

9.2 Data protection by design and by default

123. As stated in Article 25 GDPR, controllers need to implement appropriate data protection technical and organisational measures as soon as they plan for video surveillance, before they start the collection and processing of video footage. These principles emphasize the need for built-in privacy enhancing technologies, default settings that minimise the data processing, and the provision of the necessary tools that enable the highest possible protection of personal data²².
124. Controllers should build data protection and privacy safeguards not only into the design specifications of the technology but also into organisational practices. When it comes to organizational practices, the controller should adopt an appropriate management framework, establish and enforce policies and procedures related to video surveillance. From the technical point of view, system specification and design should include requirements for processing personal data in accordance with principles stated in Article 5 GDPR (lawfulness of processing, purpose and data limitation, data minimisation by default in the sense of Article 25 (2) GDPR, integrity and confidentiality, accountability etc.). In case a controller plans to acquire a commercial video surveillance system, the controller needs to include these requirements in the purchase specification. The controller needs to ensure compliance with these requirements applying them to all components of the system and to all data processed by it, during their entire lifecycle.

9.3 Concrete examples of relevant measures

125. Most of the measures that can be used to secure video surveillance, especially when digital equipment and software are used, will not differ from those used in other IT systems. However, regardless of the solution selected, the controller must adequately protect all components of a video surveillance

22 WP Opinion 168 on the "The Future of Privacy", joint contribution by the Article 29 Data Protection Working Party and the Working Party on Police and Justice to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (adopted on 01 December 2009), https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

system and data under all stages, i.e., during storage (data at rest), transmission (data in transit) and processing (data in use). For this, it is necessary that controllers and processors combine organizational and technical measures.

126. When selecting technical solutions, the controller should consider privacy-friendly technologies also because they enhance security. Examples of such technologies are systems that allow masking or scrambling areas that are not relevant to surveillance, or the editing out of images of third persons, when providing video footage to data subjects.²³ On the other hand, the selected solutions should not provide functions that are not necessary (e.g., unlimited movement of cameras, zoom capability, radio transmission, analysis and audio recordings). Functions provided, but not necessary, must be deactivated.
127. There is a lot of literature available on this subject, including international standards and technical specifications on the physical security of multimedia systems²⁴, and the security of general IT systems²⁵. Therefore, this section provides only a high-level overview of this topic.

9.3.1 Organisational measures

128. Apart from a potential DPIA needed (see section 10), controllers should consider the following topics when they create their own video surveillance policies and procedures:

-) Who is responsible for management and operation of the video surveillance system
-) Purpose and scope of the video surveillance project
-) Appropriate and prohibited use (where and when video surveillance is allowed and where and when it is not; e.g. use of hidden cameras and audio in addition to video recording²⁶)
-) Transparency measures as referred to in section 7 (Transparency and information obligations)
-) How video is recorded and for what duration, including archival storage of video recordings related to security incidents
-) Who must undergo relevant training and when
-) Who has access to video recordings and for what purposes
-) Operational procedures (e.g. by whom and from where video surveillance is monitored, what to do in case of a data breach incident)
-) What procedures external parties need to follow in order to request video recordings, and procedures for denying or granting such requests
-) Procedures for VSS procurement, installation and maintenance
-) Incident management and recovery procedures.

23 The use of such technologies may be even mandatory in some cases to comply with Article 5 (1) (c). In any case they can serve as best practice examples.

24 IEC TS 62045 — Multimedia security - Guideline for privacy protection of equipment and systems in and out of use

25 ISO/IEC 27000 — Information security management systems series

26 This may depend on national laws and sector regulations

9.3.2 Technical measures

129. **System security** means **physical security** of all system components, system integrity i.e. **protection against and resilience under intentional and unintentional interference with its normal operations** and **access control**. Data security means **confidentiality** (data is accessible only to those who are granted access), **integrity** (prevention against data loss or manipulation) and **availability** (data can be accessed when it is required).
130. **Physical security** is a vital part of data protection and the first line of defence, because it protect VSS equipment from theft, vandalism, natural disaster, manmade catastrophes and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). In case of an analogue based systems, physical security plays the main role in their protection.
131. **System and data security**, i.e. protection against intentional and unintentional interference with its normal operations may include:
-) Protection of the entire VSS infrastructure (including remote cameras, cabling and power supply) against physical tampering and theft
 -) Protection of footage transmission with communication channels secure against interception
 -) Data encryption
 -) Use of hardware and software based solutions such as firewalls, antivirus or intrusion detection systems against cyber attacks
 -) Detection of failures of components, software and interconnections
 -) Means to restore availability and access to the system in the event of a physical or technical incident.

Access control ensures that only authorized people can access the system and data, while others are prevented from doing it. Measures that support physical and logical access control include:

-) Ensuring that all premises where monitoring of video surveillance is done and video footage is stored are secured against unsupervised access by third parties
-) Positioning monitors in such a way (especially when they are in open areas, like a reception) so that only authorized operators can view them
-) Procedures for granting, changing and revoking physical and logical access are defined and enforced.
-) Methods and means of user authentication and authorization including e.g. passwords length and change frequency are implemented.
-) User performed actions (both to the system and data) are recorded and regularly reviewed.
-) Monitoring and detection of access failures is done continuously and identified weaknesses are addressed as soon as possible.

10 DATA PROTECTION IMPACT ASSESSMENT

132. According to Article 35 (1) GDPR controllers are required to conduct data protection impact assessments (DPIA) when a type of data processing is likely to result in a high risk to the rights and

freedoms of natural persons. Article 35 (3) (c) GDPR stipulates that controllers are required to carry out data protection impact assessments if the processing constitutes a systematic monitoring of a publicly accessible area on a large scale. Moreover, according to Article 35 (3) (b) GDPR a data protection impact assessment is also required when the controller intends to process special categories of data on a large scale.

133. The Guidelines on Data Protection Impact Assessment²⁷ provide further advice, and more detailed examples relevant to video surveillance (e.g., concerning the “use of a camera system to monitor driving behaviour on highways”). Article 35 (4) GDPR requires that each supervisory authority publish a list of the kind of processing operations that are subject to mandatory DPIA within their country. These lists can be usually found on the authorities’ websites. Given the typical purposes of video surveillance (protection of people and property, detection, prevention and control of offences, collection of evidence and biometric identification of suspects), it is reasonable to assume that many cases of video surveillance will require a DPIA. Therefore, data controllers should carefully consult these documents in order to determine whether such an assessment is required and conduct it if necessary. The outcome of the performed DPIA should determine the controller’s choice of implemented data protection measures.
134. It is also important to note that if the results of the DPIA indicate that processing would result in a high risks despite security measures planned by the controller, then it will be necessary to consult the relevant supervisory authority prior to the processing. Details on prior consultations can be found in Article 36.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

27 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01, http://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=611236

This page is intentionally left blank

COMMUNITY WELL BEING PDG

20TH AUGUST 2019

REPORT OF THE HEAD OF PLANNING, ECONOMY AND REGENERATION

COMMUNITIES TOGETHER FUND SUMMARY OF SPEND AND OVERVIEW OF CHANGES TO LOCAL FUNDING SCHEMES

Cabinet Member Cllr Dennis Knowles
Responsible Officer Mrs Jenny Clifford, Head of Planning, Economy and Regeneration

Reason for Report: To provide Members with a summary of spend for the Communities Together Fund (2018/19) and to inform them of the closure of the funding scheme for 2019/20.

RECOMMENDATION(S): That the report is noted.

Relationship to Corporate Plan: The report relates to Aim 1 of the Community Priority 'Support local communities to retain and develop their local facilities and services'.

Financial Implications: The Council contributed £0.10 per elector, amounting to £6,788 for the financial year 2018/19 based on the February 2018 electoral register. Mid Devon District Council administered the scheme on behalf of Devon County Council. The amount of time needed to respond to enquiries, receive and process applications, convene meetings of the County Committee and process payments has amounted to at least 20 days of officer time per year.

Legal Implications: Failure to have an efficient and effective process in place for administering the Communities Together Fund could result in legal challenge and adverse publicity for the Council.

Risk Assessment: Failure to have an efficient and effective process in place for administering the Communities Together Fund and other similar funding schemes could result in legal challenge and adverse publicity for the Council.

1.0 Introduction

- 1.1 In 2012 the County Council and District Councils created a joint grant programme, called the Town and Parish (TAP) Fund. The aim of the fund was to encourage towns and parishes to work together on mutually beneficial projects. The funding pot consisted of a contribution of £1.00 per elector from Devon County Council with the addition of £0.10 per elector from each District Council, amounting in Mid Devon in 2018 to a grant pot of just under £68,000.
- 1.2 The Fund was administered at district level with applications being approved by a panel consisting of the relevant Devon County Councillors plus two Mid Devon District Councillors. County Members had the casting vote for applications within their ward.

- 1.3 For the financial year 2018-19 the TAP Fund was rebranded the Communities Together Fund (CTF), with the aim of encouraging more applications from community groups, working together on mutually beneficial projects. In the spring of 2019 Devon County Council announced they were going to discontinue the Communities Together Fund for the financial year 2019-20, in favour of supporting three new funding schemes. The Communities Together Fund is now therefore closed to applications.
- 1.4 This report summarises the fund activities and spend for the financial year 2018-19 with a list of all applications received and grants approved attached. It then goes on to outline future arrangements for groups wanting to access DCC funding.

2.0 Communities Together Fund 2018/19 - Summary of Spend

- 2.1 The total budget for 2018/19, including both the DCC and MDDC contributions, was £67,881.00. An additional £1,068.29 of funding became available from withdrawn applications from the previous funding year. The total funding available was split between two funding rounds, of which a total of £68,949.29 was allocated, underspends in County ward areas were redistributed with County Member consent to ensure the fund was fully spent by the end of the financial year. The spend profile was as follows:

County Ward	TOTAL Budget for Year	Allocated in Round 1	Allocated in Round 2	Total allocated	Outstanding Balance
Crediton	£11,097.90	£1,333.00	£5,726.67	£7,059.67	£4,038.23
Creedy, Taw and Mid Exe	£11,679.80	£4,844.00	£13,736.03	£18,580.03	-£6,900.23
Cullompton and Bradninch	£10,808.60	£2,900.00	£7,908.60	£10,808.60	£0.00
Tiverton East	£10,692.00	£0.00	£8,782.92	£8,782.92	£1,909.08
Tiverton West	£11,919.60	£0.00	£10,419.60	£10,419.60	£1,500.00
Willand and Uffculme	£11,683.10	£4,346.80	£8,951.67	£13,298.47	-£1,615.37
Underspend	£1,068.29	£0.00	£0.00	£0.00	£1,068.29
TOTAL	£68,949.29	£13,423.8	£55,525.49	£68,949.29	£0.00

- 2.2 Appendix A outlines the 2018/19 summary of spend per County Ward.
- 2.3 We received a total of 77 applications and enquiries in 2018/19 and an additional 2 applications that had been carried forward from 2017/18. Of these 79, 21 did not proceed past the enquiry / initial application stage (the applicants either did not proceed with making a formal application for funding or withdrew their application).
- 2.5 Of the 58 applications that proceeded to Funding Panels:
- 13 were received in Round 1 and 45 were received in Round 2.

- 47 applications (81%) were successful in being allocated funding (2 of which were conditional awards) plus an additional 4 applications (7%) successfully received S106 funding instead of Communities Together Funding.
- 2 applications were deferred (carried forward from Round 1 to Round 2, which then successfully received funding).
- 7 applications (12%) were declined either due to the application not meeting the Communities Together Fund criteria or due to inadequate funding during that round. This is a 1% increase on the previous year.

2.6 Successful applicants have until 28 February 2020 to claim their funding. Any unclaimed funds will be offered to projects that only received part funding (to be selected by the County Ward Members).

3.0 Devon County Council Funding Schemes for 2019/20

3.1 In March 2019, Devon County Council announced the decision to discontinue the Communities Together Fund in the 2019/20 financial year. Instead, they are administering three separate funding schemes:

- **Crowdfund Devon (Extra funding for Devon)** Further details are on the Crowdfunder website: <https://welcome.crowdfunder.co.uk/crowdfund-devon/>
- **Doing What Matters (Community Grants Fund)** featuring an intervention rate of 75% (25% match required) - offering one-off grants of between £5k to £20k to successful community project applicants: <https://www.devon.gov.uk/economy/business-support/doing-what-matters-communities-grants-fund/>
- **Making the Connection** grant fund - deploying one-off grants of up to £300 with no match funding required: <https://www.devon.gov.uk/communities/making-the-connection-grant>

Contact for more Information: Zoë Lentell, Growth and Regeneration Officer ext 4298

Circulation of the Report:

List of Background Papers:

Appendix A: Summary of Decisions Round 1, 2018/19 by County Ward
Appendix B: Summary of Decisions Round 2, 2018/19 by County Ward

This page is intentionally left blank

COMMUNITIES TOGETHER FUND: SUMMARY OF DECISIONS
2018/19 ROUND 1 FUNDING (DEADLINE 30 SEPTEMBER 2018)

CREDITON							
REF	LEAD APPLICANT	PROJECT	PARISH	£ REQUESTED	DECISION	£APPROVED	NOTES
R1-18/19-10	CREDITON METHODIST CHURCH	CREDITON REPAIR CAFÉ	CREDITON	£ 970.00	FUND in FULL	£ 970.00	
R1-18/19-13	CREDITON TOWN COUNCIL	TRAFFIC CONES FOR COMMUNITY EVENTS	CREDITON	£ 363.00	FUND in FULL	£ 363.00	
TOTAL REQUESTED				£ 1,333.00	BUDGET AVAILABLE	£ 5,548.95	
					TOTAL AWARDED	£ 1,333.00	
					CARRY FORWARD	£ 4,215.95	

CREEDY, TAW & MID EXE							
REF	LEAD APPLICANT	PROJECT	PARISH	£ REQUESTED	DECISION	£AWARDED	NOTES
R1-18/19-01	THORVERTON PARISH COUNCIL	DEVON AIR AMBULANCE TRUST HELICOPTER NIGHT LANDING SITE	THORVERTON	£ 1,459.00	FUND in FULL	£ 1,459.00	
R1-18/19-03	CHAWLEIGH PLAYING FIELD COMMITTEE	OUTDOOR TABLE TENNIS TABLES	CHAWLEIGH	£ 650.00	DEFER	£ -	RECOMMEND APPLICANT SEEKS S106 FUNDING FIRST
R1-18/19-07	DOWN ST MARY PARISH COUNCIL	SCHOOL BUS SHELTER	DOWN ST MARY	£ 1,890.00	FUND in FULL	£ 1,890.00	
R1-18/19-09	BLACKDOG MEMORIAL HALL	DEFIBRILLATOR	WASHFORD PYNE	£ 1,495.00	FUND in FULL	£ 1,495.00	
TOTAL REQUESTED				£ 5,494.00	BUDGET AVAILABLE	£ 5,839.90	
					TOTAL AWARDED	£ 4,844.00	
					CARRY FORWARD	£ 995.90	

CULLOMPTON & BRADNINCH							
REF	LEAD APPLICANT	PROJECT	PARISH	£ REQUESTED	DECISION	£APPROVED	NOTES
R1-18/19-08	BRADNINCH 12TH NIGHT GROUP	12TH NIGHT LANTERN EVENT	BRADNINCH	£ 400.00	FUND in FULL	£ 400.00	
R1-18/19-11	CULLOMPTON WALRONS PRESERVATION TRUST	PURCHASE OF PA SYSTEM	CULLOMPTON	£ 500.00	FUND in FULL	£ 500.00	
R1-18/19-12	BRADNINCH YOUTH FOOTBALL CLUB	NEW CHANGING ROOM FACILITIES	BRADNINCH	£ 2,000.00	FUND in FULL	£ 2,000.00	ADVISE APPLICANT TO ALSO SEEK S106 FUNDING FOR TRAINING EQUIP
TOTAL REQUESTED				£ 2,900.00	BUDGET AVAILABLE	£ 5,404.30	
					TOTAL AWARDED	£ 2,900.00	
					CARRY FORWARD	£ 2,504.30	

TIVERTON EAST							
REF	LEAD APPLICANT	PROJECT	PARISH	£ REQUESTED	DECISION	£APPROVED	NOTES
	(NO APPLICATIONS THIS ROUND)						
TOTAL REQUESTED				£ -	BUDGET AVAILABLE	£ 5,346.00	
					TOTAL AWARDED	£ -	
					CARRY FORWARD	£ 5,346.00	

TIVERTON WEST							
REF	LEAD APPLICANT	PROJECT	PARISH	£ REQUESTED	DECISION	£APPROVED	NOTES
R1-18/19-06	RIVERSIDE HALL	AUTOMATED ENTRANCE DOOR	BAMPTON	£ 2,500.00	DEFER	£ -	CONDITION: APPLICANT PROVIDES ADDITIONAL EVIDENCE AS REQUESTED
TOTAL REQUESTED				£ 2,500.00	BUDGET AVAILABLE	£ 5,959.80	
					TOTAL AWARDED	£ -	
					CARRY FORWARD	£ 5,959.80	

WILLAND AND UFFCULME							
REF	LEAD APPLICANT	PROJECT	PARISH	£ REQUESTED	DECISION	£APPROVED	NOTES
R1-18/19-02	WILLAND PARISH COUNCIL	JUBILEE FIELD ENHANCEMENT - PROVISION OF SEATING	WILLAND	£ 3,214.80	Fund in FULL with CONDITIONS	£ 1,964.80	RECOMMEND DIFFERENCE IS FUNDED VIA S106
R1-18/19-04	HEMYOCK PARISH COUNCIL	NOTICEBOARDS	HEMYOCK	£ 5,300.00	Fund in PART	£ 2,382.00	
R1-18/19-05	CLAY LINE PIGS COOPERATIVE	CLAY LANE PIGS	UFFCULME	£ 714.34	DO NOT FUND	£ -	PROJECT DID NOT MEET CRITERIA FOR FUND
TOTAL REQUESTED				£ 6,014.34	BUDGET AVAILABLE	£ 5,841.55	
					TOTAL AWARDED	£ 4,346.80	
					CARRY FORWARD	£ 1,494.75	

2018/19 ROUND 1 SUMMARY						
BUDGET AVAILABLE		AWARDED				
Underspend	0.00	Underspend	0.00	<i>Underspend is returned funding from withdrawn projects from previous rounds/years</i>		
Crediton	5,548.95	Crediton	1,333.00			
Creedy, Taw and Mid Ex	5,839.90	Creedy, Taw and Mid Exe	4,844.00			
Cullompton and Bradninch	5,404.30	Cullompton and Bradninch	2,900.00			
Tiverton East	5,346.00	Tiverton East	0.00			
Tiverton West	5,959.80	Tiverton West	0.00			
Willand and Uffculme	5,841.55	Willand and Uffculme	4,346.80			
TOTAL BUDGET	33,940.50	TOTAL AWARDED	13,423.80			
		REMAINING BALANCE	20,516.70			

This page is intentionally left blank

COMMUNITIES TOGETHER FUND: SUMMARY OF DECISIONS
2018/19 ROUND 2 FUNDING (DEADLINE 21 FEBRUARY 2019)

REF	APPLICANT	PROJECT	PARISH	£ REQUESTED	DECISION	£ AWARDED	NOTES
R2-18/19-09	YEOFORD COMMUNITY ASSOCIATION	YEOFORD COMMUNITY GARDEN	CREDITON HAMLETS	£ 1,060.00	FUND IN FULL	£ 1,060.00	
R2-18/19-11	CREDITON TOWN TEAM	EXTENDING PARTICIPATION IN CREDFEST 19	CREDITON	£ 2,000.00	FUND IN PART	£ 1,450.00	FUNDING TOWARDS THE BIG READ AND PICNIC IN THE PARK
R2-18/19-12	CREDITON CONGREGATIONAL CHURCH	CHURCHYARD PROJECT	CREDITON	£ 1,500.00	FUND IN FULL	£ 1,500.00	
R2-18/19-19	TIVERTON TIS	VISIT MID DEVON	ALL	£ 716.67	FUND IN FULL	£ 716.67	JOINT APPLICATION: TOTAL FUNDED = £3,941.69
R2-18/19-44	THE TURNING TIDES PROJECT	ANOTHER ROOT - SUPPORTED GARDENING SCHEME	CREDITON	£ 1,000.00	FUND IN FULL	£ 1,000.00	
TOTAL REQUESTED				£ 6,276.67	BUDGET AVAILABLE	£ 9,764.90	
					TOTAL AWARDED	£ 5,726.67	
					REMAINING BALANCE	£ 4,038.23	

REF	APPLICANT	PROJECT	PARISH	£ REQUESTED	DECISION	£ AWARDED	NOTES
R1-18/19-03	CHAWLEIGH PLAYING FIELD COMMITTEE	OUTDOOR TABLE TENNIS TABLES	CHAWLEIGH	£ 650.00	DO NOT FUND	£ -	RECOMMEND: FUND THROUGH S106
R2-18/19-05	COLDRIDGE PARISH COUNCIL	REFURBISHMENT OF VILLAGE HALL	COLDRIDGE	£ 500.00	FUND IN FULL	£ 500.00	
R2-18/19-06	SHOBROOKE PC	GRIT BINS	SHOBROOKE	£ 279.00	CONDITIONAL FUND IN FULL	£ 279.00	CONDITION: HIGHWAYS PERMISSION
R2-18/19-19	TIVERTON TIS	VISIT MID DEVON	ALL	£ 716.67	FUND IN FULL	£ 716.67	JOINT APPLICATION: TOTAL FUNDED = £3,941.69
R2-18/19-26	CADELEIGH VILLAGE HALL	STORAGE SHED	CADELEIGH	£ 1,000.00	FUND IN PART	£ 500.00	
R2-18/19-27	THELBRIDGE PARISH HALL	FIRE DOOR	THELBRIDGE	£ 400.00	FUND IN FULL	£ 400.00	
R2-18/19-31	LAPFORD / CRUWYS MORCHARD / DOWN ST MARY	ESTABLISHMENT OF A TRAFFIC ORDER REGULATION	MULTIPLE	£ 2,700.00	FUND IN PART	£ 2,200.00	
R2-18/19-32	THORVERTON PARISH COUNCIL	COMMUNITY ARCHAEOLOGICAL DIG	THORVERTON	£ 5,000.00	FUND IN PART	£ 2,500.00	
R2-18/19-34	SANDFORD PARISH COUNCIL	PLAY AREA	SANDFORD	£ 2,000.00	FUND IN FULL	£ 2,000.00	
R2-18/19-40	KENNERLEIGH COMMUNITY SHOP	EXTENSION TO COMMUNITY SHOP	KENNERLEIGH	£ 3,300.00	FUND IN PART	£ 2,000.00	
R2-18/19-42	THORVERTON PARISH COUNCIL	MOWER	THORVERTON	£ 2,500.00	FUND IN PART	£ 1,250.00	
R2-18/19-43	LIGHTHOUSE HOLIDAY CLUB	MAY 2019 HOLIDAY CLUB	MORCHARD BISHOP	£ 1,554.63	FUND IN PART	£ 1,390.36	
TOTAL REQUESTED				£ 20,600.30	BUDGET AVAILABLE	£ 6,835.80	
					TOTAL AWARDED	£ 13,736.03	
					REMAINING BALANCE	-£ 6,900.23	

REF	APPLICANT	PROJECT	PARISH	£ REQUESTED	DECISION	£ AWARDED	NOTES
R2-18/19-13	BRADNINCH FIREWORKS NIGHT GROUP	FIREWORK EVENT	BRADNINCH	£ 450.00	FUND IN FULL	£ 450.00	
R2-18/19-14	SUSTAINABLE BRADNINCH	BRADNINCH REPAIR CAFE	BRADNINCH	£ 600.00	FUND IN FULL	£ 600.00	
R2-18/19-15	COMMUNITY LIFE HUB (CULLOMPTON)	GARDEN PROJECT	CULLOMPTON	£ 3,100.00	FUND IN PART	£ 996.00	RECOMMEND DIFFERENCE IS FUNDED THROUGH S106
R2-18/19-16	CULLOMPTON TOWN TEAM	CULLOMPTON HIGH STREET FESTIVALS	CULLOMPTON	£ 1,500.00	FUND IN PART	£ 1,000.00	
R2-18/19-17	CULLOMPTON TOWN COUNCIL	LEAT BARRIER	CULLOMPTON	£ 1,000.00	DO NOT FUND	£ -	
R2-18/19-18	CULLOMPTON WALRONS PRESERVATION TRUST	INTERPRETATION BOARDS	CULLOMPTON	£ 5,000.00	FUND IN PART	£ 2,639.26	
R2-18/19-19	TIVERTON TIS	VISIT MID DEVON	ALL	£ 716.67	FUND IN PART	£ 358.34	JOINT APPLICATION: TOTAL FUNDED = £3,941.69
R2-18/19-20	BLACKBOROUGH VILLAGE HALL	DISHWASHER	KENTISBEARE	£ 750.00	FUND IN FULL	£ 750.00	
R2-18/19-21	BRADNINCH TOWN COUNCIL	RECYCLING BINS	BRADNINCH	£ 1,190.00	FUND IN PART	£ 800.00	
R2-18/19-23	CULLOMPTON TOWN COUNCIL	FLAGPOLES	CULLOMPTON	£ 690.00	DO NOT FUND	£ -	
R2-18/19-24	CULLOMPTON TOWN COUNCIL	TOWN LEAT HANDRAIL	CULLOMPTON	£ 500.00	DO NOT FUND	£ -	
R2-18/19-41	BUTTERLEIGH PARISH MEETING	NOTICEBOARD	BUTTERLEIGH	£ 315.00	FUND IN FULL	£ 315.00	
TOTAL REQUESTED				£ 15,811.67	BUDGET AVAILABLE	£ 7,908.60	
					TOTAL AWARDED	£ 7,908.60	
					REMAINING BALANCE	£ -	

REF	APPLICANT	PROJECT	PARISH	£ REQUESTED	DECISION	£ AWARDED	NOTES
R2-18/19-02	TAPA	JOINT SCHOOL HOLIDAY PROJECT	TIVERTON TOWN	£ 2,000.00	FUND IN FULL	£ 2,000.00	JOINT APPLICATION: TOTAL FUNDED = £4,000.00
R2-18/19-03	TIVERTON ROTARY CLUB	TIVERTON LEAT ENHANCEMENT	TIVERTON TOWN	£ 3,750.00	DO NOT FUND	£ -	RECOMMEND FUND THROUGH S106
R2-18/19-04	HALBERTON PARISH COUNCIL	NEW PICNIC TABLES	HALBERTON	£ 850.00	DO NOT FUND	£ -	RECOMMEND FUND THROUGH S106
R2-18/19-07	MID DEVON MOBILITY	OPTIMISING DATA PROTECTION	TIVERTON TOWN	£ 1,350.00	DO NOT FUND	£ -	RECOMMEND DCC LOCALITY BUDGET (TIVERTON EAST AND WEST)
R2-18/19-19	TIVERTON TIS	VISIT MID DEVON	ALL	£ 716.67	FUND IN FULL	£ 716.67	JOINT APPLICATION: TOTAL FUNDED = £3,941.69
R2-18/19-28	TIVERTON TERRIERS	YOUTH NETBALL SQUAD	YOUTH NETBALL SQUAD	£ 985.55	FUND IN PART	£ 637.25	RECOMMEND DIFFERENCE IS FUNDED VIA S106
R2-18/19-30	BOUNCE! BRIGHTER FUTURES FOUNDATION	PILOT PHASE	TIVERTON TOWN	£ 2,193.75	FUND IN PART	£ 2,700.00	JOINT APPLICATION: TOTAL FUNDED = £3,803.88
R2-18/19-33	TIVERTON TOWN ABILITY COUNTS FC	MINI-BUS HIRE FOR CELEBRATION EVENT	TIVERTON TOWN	£ 175.00	FUND IN FULL	£ 175.00	JOINT APPLICATION: TOTAL FUNDED = £350.00
R2-18/19-35	DAISI	200 YEARS OF TIVERTON	TIVERTON TOWN	£ 1,000.00	FUND IN FULL	£ 1,000.00	JOINT APPLICATION: TOTAL FUNDED = £2,000.00
R2-18/19-37	DOGS HELPING KIDS	EXPANDING TO ALL MID DEVON	ALL	£ 1,800.00	FUND IN PART	£ 1,054.00	
R2-18/19-45	AFFINITY SUPPORT GROUP	SUMMER ACTIVITIES 2019	TIVERTON TOWN	£ 3,268.64	CONDITIONAL FUND IN PART	£ 500.00	CONDITION: CLARIFICATION OF STATUS OF PREVIOUS AWARD
TOTAL REQUESTED				£ 18,089.60	BUDGET AVAILABLE	£ 10,692.00	
					TOTAL AWARDED	£ 8,782.92	
					REMAINING BALANCE	£ 1,909.08	

REF	APPLICANT	PROJECT	PARISH	£ REQUESTED	DECISION	£ AWARDED	NOTES
R1-18/19-06	RIVERSIDE HALL	AUTOMATED ENTRANCE DOOR	BAMPTON	£ 2,500.00	FUND IN FULL	£ 2,500.00	
R2-18/19-01	MID DEVON SHOW	YOUTH VILLAGE	TIVERTON TOWN	£ 2,000.00	DO NOT FUND	£ -	
R2-18/19-02	TAPA	JOINT SCHOOL HOLIDAY PROJECT	TIVERTON TOWN	£ 2,000.00	FUND IN FULL	£ 2,000.00	JOINT APPLICATION: TOTAL FUNDED = £4,000.00
R2-18/19-03	TIVERTON ROTARY CLUB	TIVERTON LEAT ENHANCEMENT	TIVERTON TOWN	£ 3,750.00	DO NOT FUND	£ -	RECOMMEND FUND THROUGH S106
R2-18/19-07	MID DEVON MOBILITY	OPTIMISING DATA PROTECTION	TIVERTON TOWN	£ 1,350.00	DO NOT FUND	£ -	RECOMMEND DCC LOCALITY BUDGET (TIVERTON EAST AND WEST)
R2-18/19-10	TIVERTON MUSEUM OF MID DEVON LIFE	MUSEUM WITHOUT WALLS	TIVERTON TOWN	£ 1,263.00	FUND IN FULL	£ 1,263.00	
R2-18/19-19	TIVERTON TIS	VISIT MID DEVON	ALL	£ 716.67	FUND IN FULL	£ 716.67	JOINT APPLICATION: TOTAL FUNDED = £3,941.69
R2-18/19-28	TIVERTON TERRIERS	YOUTH NETBALL SQUAD	TIVERTON TOWN	£ 985.55	FUND IN PART	£ 637.25	RECOMMEND DIFFERENCE IS FUNDED VIA S106
R2-18/19-29	TIVERTON UNITED CHURCH (METHODIST AND UR)	CCTV	TIVERTON TOWN	£ 523.80	FUND IN FULL	£ 523.80	
R2-18/19-30	BOUNCE! BRIGHTER FUTURES FOUNDATION	PILOT PHASE	TIVERTON TOWN	£ 2,193.75	FUND IN PART	£ 1,103.88	JOINT APPLICATION: TOTAL FUNDED = £3,803.88
R2-18/19-33	TIVERTON TOWN ABILITY COUNTS FC	MINI-BUS HIRE FOR CELEBRATION EVENT	TIVERTON TOWN	£ 175.00	FUND IN FULL	£ 175.00	JOINT APPLICATION: TOTAL FUNDED = £350.00
R2-18/19-35	DAISI	200 YEARS OF TIVERTON	TIVERTON TOWN	£ 1,000.00	FUND IN FULL	£ 1,000.00	JOINT APPLICATION: TOTAL FUNDED = £2,000.00
R2-18/19-38	MOREBATH CRICKET CLUB	REPLACEMENT TO BOUNDARY FENCE	MOREBATH	£ 7,414.88	DO NOT FUND	£ -	RECOMMEND FUND THROUGH S106
R2-18/19-45	AFFINITY SUPPORT GROUP	SUMMER ACTIVITIES 2019	TIVERTON TOWN	£ 3,268.64	FUND IN PART	£ 500.00	CONDITION: CLARIFICATION OF STATUS OF PREVIOUS AWARD
TOTAL REQUESTED				£ 29,141.28	BUDGET AVAILABLE	£ 11,919.60	
					TOTAL AWARDED	£ 10,419.60	
					REMAINING BALANCE	£ 1,500.00	

REF	APPLICANT	PROJECT	PARISH	£ REQUESTED	DECISION	£ AWARDED	NOTES
R2-18/19-08	UFFCULME VILLAGE HALL	REFURBISHMENT OF VILLAGE HALL	UFFCULME	£ 1,235.00	FUND IN FULL	£ 1,235.00	
R2-18/19-19	TIVERTON TIS	VISIT MID DEVON	ALL	£ 716.67	FUND IN FULL	£ 716.67	JOINT APPLICATION: TOTAL FUNDED = £3,941.69
R2-18/19-22	CLAYHIDON VILLAGE HALL	PARISH HALL IMPROVEMENTS	CLAYHIDON	£ 6,809.00	FUND IN PART	£ 3,000.00	
R2-18/19-25	UFFCULME BOWLING CLUB	ENTRANCE GATE RELOCATION	UFFCULME	£ 800.00	DO NOT FUND	£ -	RECOMMEND FUND THROUGH S106
R2-18/19-36	UFFCULME PARISH COUNCIL	WATER DRINKER	UFFCULME	£ 1,000.00	FUND IN FULL	£ 1,000.00	
R2-18/19-39	UFFCULME SCHOOL	ASTRO PROJECT	UFFCULME	£ 10,000.00	FUND IN PART	£ 3,000.00	
TOTAL REQUESTED				£ 20,560.67	BUDGET AVAILABLE	£ 7,336.30	
					TOTAL AWARDED	£ 8,951.67	
					REMAINING BALANCE	-£ 1,615.37	

SUMMARY		BUDGET AVAILABLE	AWARDED	NOTES
	Underspend	1,068.29	Underspend	0.00
	Crediton	9,764.90	Crediton	5,726.67
	Creedy, Taw and Mid Exe	6,835.80	Creedy, Taw and Mid Exe	13,736.03
	Culompton and Bradninch	7,908.60	Culompton and Bradninch	7,908.60
	Tiverton East	10,692.00	Tiverton East	8,782.92
	Tiverton West	11,919.60	Tiverton West	10,419.60
	Willand and Uffculme	7,336.30	Willand and Uffculme	8,951.67
	TOTAL BUDGET	55,525.49	TOTAL AWARDED	55,525.49
			REMAINING BALANCE	0.00

This page is intentionally left blank

**COMMUNITY PDG
20 AUGUST 2019**

REGULATION OF INVESTIGATORY POWERS ACT (RIPA) POLICY AND PROCEDURES 2019

Cabinet Member(s): Cllr Nikki Woollatt, Cabinet Member for the Working Environment and Support Services
Responsible Officer: Director of Corporate Affairs and Business Transformation

Reason for Report: to undertake the annual review of the Council's existing RIPA policy; to inform Members of the use of RIPA powers by the Council; to consider whether officers should draft a policy on covert surveillance for non-RIPA cases; and to inform Members of the intention to roll out training to officers on the monitoring of information online such as social media posts

RECOMMENDATIONS:

- (1) that it is recommended to Cabinet to approve the revised RIPA Policy, including the new Annex 1 on social media/internet research;
- (2) that officers draft a policy on covert surveillance for non-RIPA cases to be submitted for approval; and
- (3) to note that the contents of the Report, including the fact that the Council has not used its powers under RIPA since March 2014 and that training will be given to officers on monitoring of information posted online, such as social media posts.

Financial Implications: None directly arising, other than officer time

Legal Implications: As set out in the policy and this report

Risk Assessment: Adopting and complying with a RIPA Policy will minimise any risk to the Council of acting unlawfully

Equality Impact Assessment: No equality issues directly arising from this report

Relationship to Corporate Plan: Statutory guidance requires elected members to review the Council's use of RIPA and approve the RIPA policy at least once a year- therefore these requirements need to be complied with to show the Council is a well-managed Council

Impact on Climate Change: None directly arising

1 Background

- 1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) was put in place to ensure that the use of certain investigatory powers by certain organisations complies with the UK's obligations under the European Convention on Human

Rights (ECHR) including Article 8 (the right to privacy). The proper authorisation of certain covert surveillance powers under RIPA ensures that the Council is acting in accordance with such human rights.

- 1.2 Following criticism of local authorities' use of covert surveillance powers additional safeguards were put in place including:-
- The need to obtain magistrate approval
 - Only be used to investigate offences which attract sentences of six months or more or relate to the underage sale of alcohol or tobacco.

2 The need for a covert surveillance policy for non-RIPA cases

- 2.1 The effect of these safeguards and restrictions mean that it will be a very rare occurrence for RIPA authorisation and judicial approval to be obtained – indeed the Council has not made use of such powers since 2014. The type of offences which the Council typically investigates does not attract sentences of six months or more. However, there may be occasions when the Council wants to conduct covert surveillance which could not be approved under RIPA because it is not an investigation into an offence which attracts a sentence of six months or more.
- 2.2 It should also be noted that covert investigation carried out without RIPA authorisation is not automatically unlawful because of the lack of authorisation. For instance if the Council conducts covert surveillance without RIPA authorisation it will not be in breach of Article 8 privacy rights if the Council can show that the interference was necessary and proportionate and there was process of authorisation that was fair.
- 2.3 The Office of Surveillance Commissioners in its Annual Report for 2012 to 2013 at paragraph 5.5 said the following:

It is not my role to encourage more or less use of covert surveillance but there are occasions when it is considered necessary and proportionate but the protection of RIPA cannot be sought. For example, covert surveillance within the residential premises of a vulnerable person may be a necessary and proportionate response but may not meet the serious crime criteria to enable authorisation for intrusive surveillance. My published guidance is supported by the Investigatory Powers Tribunal in the case of BA and others v Cleveland Police (IPT/11/129/CH). Though less frequent there may be occasions when a local authority deem it necessary and proportionate to conduct covert surveillance which does not meet the six month criteria set out in the relevant Act. In all of these circumstances since I do not decide whether the decision is correct or the authorisation valid, I consider it wise to have a verifiable audit similar to the process and documentation for RIPA available for later scrutiny

- 2.4 Officers seek Members' agreement to develop a policy for covert surveillance where RIPA does not apply. This policy should set out the authorisation procedure which would mirror the RIPA policy, but there would not be a judicial review mechanism. This policy would set out stringent tests for authorisation similar to RIPA authorisation and it would have to take into

account the Data Protection issues and well as Human Rights considerations. Once the policy has been formulated it would be brought back before Members for approval.

3 Approval for amendments to the Council's RIPA policy

- 3.1 The Investigatory Powers Commissioner's Office (IPCO) provides independent oversight of the use of investigatory powers. It carries out periodic inspections every 3 years. The IPCO wrote to the Council on the 18th October 2018 (Appendix 1) after it carried out a "desktop based documentary inspection" by one of the inspectors. IPCO was grateful that the Council had facilitated the process enabling the inspection to be conducted by way of a "desk top" approach. The IPCO was also pleased that the level of compliance shown by the Council with RIPA was such that a physical inspection was not necessary at the present time.
- 3.2 The IPCO reviewed the Council's RIPA policy and suggested amendments along the following lines:-
1. The policy should indicate that the renewal of directed surveillance or covert human intelligence source (CHIS) authorisation must be approved by a magistrates' court in the same manner as the initial authorisation
 2. Authorisation for vulnerable persons/juveniles as CHIS or for directed surveillance where there is a risk of obtaining confidential information may only be granted by the person who has been formally nominated as the acting Chief Executive in the absence of the Chief Executive
 3. There is a need for guidance on the monitoring of information online such as social media posts, during investigations.
- 3.3 Officers have drafted amendments to the Council's RIPA policy to take into account the IPCO's comments. Suggested amendments for nos. 1 and 2 above are technical changes which do not require much in the way of comment. Suggested amendment for no. 3 above is contained in the draft Annex 1 to the RIPA policy. The revised policy with tracked changes is shown at Appendix 2 to this Report.
- 3.4 For clarity, much of the publicly accessible internet content can be accessed by officers without the need for RIPA authorisation, but in some cases RIPA authorisation is required. Unfortunately the point at which access strays into surveillance is not always clear-cut. The Government has issued a code of practice for Covert surveillance and covert human intelligence sources in order to assist compliance with RIPA. The following paragraphs at 3.10 to 3.15 of the code of practice for directed surveillance put into context the use of the internet and RIPA:

3.10. The growth of the internet and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in

preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation: use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

3.11 The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

3.12 In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available

3.13 As set out in paragraph 3.14 below, depending on the nature of the online platform there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for covert purposes such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings

3.14 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information.

Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information

3.15 Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. See also paragraph 3.6

- 3.5 The need to consider how the Council uses social media as an investigatory tool was further emphasised in expert training to key senior council officers in November 2018. Officers have therefore drafted an annex to the RIPA policy to provide guidance on the monitoring of information online such as social media posts. It is considered that training will need to be given to officers on the monitoring of information online, such as social media posts.

4 Other RIPA related activity in 2018-19

- 4.1 In addition to the review carried out by the IPCO (see paragraph 3.1 above) and the training provided in November 2018, the Co-ordinating Officer has also provided the annual statistical return to the IPCO. Thankfully, this was straightforward, given the non-use of RIPA in the previous year.

Contact for more Information: Philip Langdon (Solicitor and RIPA Co-ordinating Officer) 01884 234204 plangdon@middevon.gov.uk; Kathryn Tebbey (Group Manager for Legal Services and Monitoring Officer as Senior Responsible Officer) 01884 234210 ktebbey@middevon.gov.uk

Circulation of the Report: Cabinet Member seen and approved yes Cllr Woollatt, Leadership Team seen and approved [yes/no]

List of Background Papers: Appendix 1 – IPCO Letter dated 18 October 2018
Appendix 2 – RIPA policy – with draft revisions and additions

This page is intentionally left blank



Investigatory Powers
Commissioner's Office

PO Box 29105, London
SW1V 1ZU

Mr Stephen Walford
Chief Executive
Mid Devon District Council
Phoenix House
Phoenix Lane
Tiverton
Devon
EX16 6PP

18th October 2018

Dear Mr Walford,

**Inspection of Mid Devon District Council
Compliance with the Regulation of Investigatory Powers Act 2000 (RIPA)**

Your Council was recently subject of a desktop based documentary inspection by one of my Inspectors, Mrs Gráinne Athorn. I am grateful to you for facilitating this through your Legal Services Manager – Kathryn Tebbey who has provided the relevant materials including a comprehensive response to our Desktop Inspection Questionnaire, a copy of the Corporate Policy on the Use of Directed Surveillance and CHIS and guidance on the use of your CCTV systems.

The information you have provided has demonstrated a much improved level of compliance from that which was demonstrated at the time of the last Inspection in April 2015. This removes, for the present, the requirement for a physical inspection. It is anticipated that this will be undertaken when your authority's next three-yearly inspection is due (approximately autumn 2021).

I note that in his Inspection Report of 2015 Assistant Surveillance Commissioner HH Norman Jones made six recommendations for action, all of which have been completed. I understand that particular comment was made in relation to the overall quality of surveillance applications and authorisations. Given that Mid Devon District Council has made no further use of these powers during the intervening period, it is not possible to test if the refresher training provided to Council officials in 2015/6 has had the effect of improving the overall quality, and thus it is my intention to keep this element under review until such a time that we visit you again.

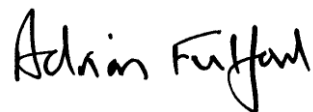
In respect of the provision of regular training, I understand that a further update package is pending and due to be delivered to key personnel in early 2019. I ask that you ensure that all four nominated Authorising Officers (including you in your capacity as Senior Authorising Officer) complete refresher training as a matter of priority to ensure that your knowledge of RIPA and the revised Codes of Practice is current.

With regard to the present corporate policy in respect of RIPA, I understand that this is due for revision shortly. Mrs Athorn has asked me to highlight three areas for improvement:

- I, Please draw readers' attention to the fact that when a directed surveillance or covert human intelligence source authorisation requires renewal, the renewal must be approved by a magistrates' court in the same manner as an initial authorisation;
- II, The policy states that in the absence of the Paid Head of Service/Chief Executive, the Corporate Directors may grant authorisations for vulnerable persons/juvenile CHIS or directed surveillance where there is a risk of obtaining confidential information. This is not the case. Such an authorisation may only be granted by the person who is formally nominated as the acting Chief Executive in your absence;
- III, It was acknowledged in your response to the desktop inspection form that there is need for guidance on the monitoring of information online such as social media posts, during investigations. I understand that the Council has already taken the stance of precluding activity of this kind, however this needs to be clearly stated within the policy.

My Office is available to you should you have any queries following the recent desktop inspection, or at any point in the future. Contact details are provided at the foot of this letter.

Yours Sincerely,

A handwritten signature in black ink that reads "Adrian Fulford". The signature is written in a cursive, slightly slanted style.

The Rt. Hon. Lord Justice Fulford
The Investigatory Powers Commissioner

MID DEVON DISTRICT COUNCIL

RIPA POLICY

USE OF DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES REGULATION OF INVESTIGATORY POWERS ACT 2000

1.0 INTRODUCTION

- 1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the use of covert investigative techniques by public authorities. It provides for the application for and granting of authorisations for those techniques covered by the Act.
- 1.2 Article 8 of the European Convention on Human Rights provides a right to private and family life. This is not an absolute right; it may be infringed in certain circumstances. The RIPA is designed to provide a statutory regulatory framework, which will meet the requirements of the European Convention on Human Rights.

2.0 PURPOSE

The purpose of this policy is to ensure that the Council complies with the requirement of RIPA and that appropriate authorisations are given for covert surveillance, the use of covert human intelligence sources and the acquisition and disclosure of communications data.

3.0 ASSOCIATED DOCUMENTS

3.1 Background documents

Report to the Council's Policy and Development Committee –15.02.01

3.2 Statutes and Statutory Instruments

- (a) Regulation of Investigatory Powers Act 2000
- (b) Human Rights Act 1998
- (c) Police and Criminal Evidence Act 1984
- (d) Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010
- (e) Protection of Freedoms Act 2012

3.3 Guidance

- (a) Explanatory Notes to RIPA
- (b) Code of Practice for covert surveillance and property interference
- (c) Code of Practice for the use of covert human intelligence sources
- (d) Code of Practice for the acquisition and disclosure of communications data
- (e) Home Office Web Site <https://www.gov.uk/guidance/surveillance-and-counter-terrorism#local-authority-use-of-ripa>

All Codes of Practice are available on the Home Office Web Site <https://www.gov.uk/government/collections/ripa-codes>

4.0 SCOPE

The Act provides a regime of primary legislation and Codes of Practice, which divide covert investigation techniques into categories distinguished to an extent by the degree of intrusion involved. This procedure applies to all investigation and surveillance that may be subject of an authorisation under RIPA.

4.1 The Act covers the following investigatory powers:

- (1) Part I (Chapter II) - the acquisition of communications related data e.g. telephone billing data
- (2) Part II deals with:
 - intrusive surveillance on residential premises or in private vehicles
 - directed surveillance i.e. covert surveillance in the course of a specific operation
 - the use of covert human intelligence sources e.g. agents, informants, undercover officers
- (3) Part III - deals with the power to seize electronic keys giving access to encrypted computer material
- (4) Part IV - provides for scrutiny, complaint procedures and codes of practice

4.2 This policy document relates to the **use of directed surveillance** and **covert human intelligence sources**. It does not cover the acquisition and disclosure of communications data as it is not anticipated that this power will be used by the Council. If authorisation is however sought for this type of activity, guidance must be sought from Legal Services before any operation or investigation is undertaken. It does not cover intrusive surveillance because local authorities are not allowed to do this. Intrusive surveillance is the covert (i.e. secret) surveillance of anything taking place in residential premises or a private car and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

4.3 RIPA sets out the purposes for which each of these powers may be used, the Agencies and authorities that can use them and who should authorise the use. Authorisation under RIPA gives lawful authority for the use of these methods of obtaining information provided there is compliance with the statutory requirements and procedures. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse. It will also make the action less vulnerable to challenge under the Human Rights Act 1998.

4.4 For district councils, the Act does not allow directed surveillance or CHIS at all except for the purpose of preventing or detecting crime or preventing disorder. For example, this means that you cannot carry out these covert activities prior to the service of a

statutory notice, unless you believe an offence may have been committed, may be about to be committed, or there could be public disorder. Your only option in other cases will be to carry out overt – open, non-secretive – surveillance.

- 4.5 Services likely to conduct investigations covered by this Act are Planning, Environmental Health, Housing and Audit. However, any officer of the Council if he or she conducts an investigation using methods or techniques covered by this Act is required to seek the necessary authorisation, provided always that the purpose of the investigation is the one which the Act says can justify covered surveillance – see 4.4 above.

5.0 ACTIVITY REQUIRING AUTHORISATION

- 5.1 The following types of activity will require authorisation:

- directed surveillance
- the conduct and use of covert human intelligence sources
- obtaining communications data

- 5.2 Directed surveillance is, in essence, any activity undertaken covertly for the purpose of a specific investigation in such a way that is likely to result in obtaining information about a person's private life.

- 5.3 A covert human intelligence sources (CHIS) is effectively an inside informant or undercover officer, i.e. someone who develops or maintains their relationship with the surveillance target, having the covert purpose of obtaining or accessing information for the investigator. Council officers may act as CHIS when undertaking social media research. For a more detailed definition see section 26 of the Act.

6.0 APPLYING FOR AUTHORISATIONS

- 6.1 Subject to the provisions of paragraphs 6.3 and 8.7 the Directors are authorising officers for the Council. In the absence of the nominated authorising officer, applications for authorisation should be submitted to Chief Executive who also has the delegated authority to issue authorisations in relation to any service of the Council. Authorising officers may authorise for any service within the Council.

- 6.2 Any officer intending to use directed surveillance or a CHIS shall apply for authorisation from the authorising officer or in their absence from the Chief Executive as Head of Paid Service or in his absence a Director who is an authorising officer by completing the appropriate application form as set out at **Appendix DS/1 or CHIS/1**.

- 6.3 Special care needs to be taken with **confidential personal information**. This is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records. This also includes legally privileged material, journalistic materials and information given to a Member of Parliament. Owing to the very sensitive nature of this type of information authorisations potentially involving confidential personal

information must always be made by the **Chief Executive** or in his/her absence the person who is formally nominated to act as the Chief Executive.

- 6.4 When completing the application always include a full account of the steps to be taken in the investigation which require authorisation.

7.0 GRANTING OF AUTHORISATIONS FOR DIRECTED SURVEILLANCE

- 7.1 Section 28 provides that a person shall not grant authorisation for *directed surveillance* unless he believes that the authorisation is necessary on one of the statutory grounds and the authorised surveillance is proportionate to what is sought to be achieved by it. The applicant and the authorising officer must both consider whether it is necessary to use covert surveillance in the investigation. From 5 January 2004, only one ground applied to district councils and it is therefore the only one which can be used to justify an authorisation.

That ground is

- for the purpose of preventing or detecting crime or of preventing disorder

- 7.2 The authorising officer in determining whether the surveillance is proportionate will give particular consideration to any collateral intrusion on or interference with the privacy of persons other than the subject(s) of the surveillance. The Home Office Code of Practice has the following to say on the issue of proportionality:

“4.5 if the activities are deemed necessary on...the statutory grounds, the person granting the authorisation... must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

4.65 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means..” Home Office Code of Practice on Covert Surveillance and Property Interference.

A useful prompt is to ask yourself “ Is there any other way of obtaining the evidence?”. There is a need to consider the following:

- (i) Whether the use of covert surveillance is proportionate to the mischief being investigated, and
- (ii) Whether it is proportionate to the likely intrusion on the target and others, and
- (iii) Whether all other reasonable means of acquiring the evidence have been considered.
- (iv) What other methods had been considered and why they were not implemented.

- 7.3 Authorisations must be given in writing. It is possible that authorising officers may face cross-examination in court about the authorisation some time after it is granted and memories fade. It is therefore important that a full written record of what you are

being asked to authorise appears on the application form. If in doubt ask for more detail.

7.4 Authorising officers should not be responsible for authorising their own activities.

7.5 All RIPA authorisations must be approved by a Magistrate before an authorisation becomes effective, directed surveillance is undertaken, communications data is obtained or an application is made for a Covert Human Intelligent Source. Directed surveillance can only be authorised where the following conditions apply;

(1) The first condition is that the authorisation under [section 28](#) is for the purpose of preventing or detecting conduct which—

(a) constitutes one or more criminal offences, or

(b) is, or corresponds to, any conduct which, if it all took place in England and Wales, would constitute one or more criminal offences.

(2) The second condition is that the criminal offence or one of the criminal offences referred to in the first condition is or would be—

(a) an offence which is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment or

are related to the underage sale of alcohol and tobacco or nicotine inhaling products.

7.6 Duration of Authorisations and Reviews

An authorisation in writing ceases to have effect at the end of a period of 3 months beginning with the day on which it took effect. So an authorisation starting 1st January would come to an end on 31st March. Regular reviews of authorisations should be undertaken. The results of the review should be recorded on **Appendix DS/2** and a copy filed on the central record of authorisations. If the surveillance provides access to confidential information or involves collateral intrusion more frequent reviews will be required. The Authorising Officer should determine how often a review should take place.

7.7 Renewals

7.7.1 While an authorisation is still effective the authorising officer can renew it if he considers this necessary for the purpose for which the authorisation was originally given. The authorisation will be renewed in writing for a further period, beginning with the day when the authorisation would have expired but for the renewal and can be for a period up to 3 months.

7.7.2 Applications requesting renewal of an authorisation are to be made on the appropriate form as set out at **Appendix DS/3** and submitted to the authorising officer. The renewal must be granted before the original authorisation ceases to have effect.

7.7.3 Applications for renewal will record:

- whether this is the first renewal, if not, every occasion on which the authorisation has previously been renewed
- the significant changes to the information in the initial authorisation

- the reasons why it is necessary to continue with the surveillance
- the content and value to the investigation or operation of the information so far obtained by the surveillance

The results of regular reviews of the investigation or operation.

7.7.4 When a directed surveillance authorisation requires renewal, the renewal must be approved by a magistrates' court in the same manner as an initial authorisation

7.8 Cancellations

The person who granted or last renewed the authorisation **MUST** cancel it if he is satisfied that the directed surveillance no longer meets the criteria for authorisation. Requests for cancellation will be made on the appropriate form as set out at **Appendix DS/4** and submitted to the authorising officer for authorisation of the cancellation. All directed surveillance cancellations must include directions for the management and storage of any surveillance product.

8.0 GRANTING OF AUTHORISATION FOR THE CONDUCT AND USE OF COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

8.1 The same requirements of necessity and proportionality exist for the granting of these authorisations as are set down for directed surveillance.

8.2 Additionally the authorising officer shall not grant an authorisation unless he /she believes that arrangements exist for the source's case which satisfy the following requirements:

- there will at all times be an officer with day to day responsibility for dealing with the source and the source's security and welfare
- there will at all times be an officer who will have general oversight of the use made of the source
- there will at all times be an officer with responsibility for maintaining a record of the information supplied by the source
- records which disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available

8.3 Similarly before authorising use or conduct of the source, the authorising officer must be satisfied that the conduct/use is proportionate to what the use or conduct of the source seeks to achieve, taking into account the likely degree of intrusion into privacy of those potentially effected for the privacy of persons other than those who are directly the subjects of the operation or investigation. Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

8.4 Particular care is required where people would expect a high degree of privacy or where, as a consequence of the authorisation 'confidential material' is likely to be obtained.

- 8.5 Consideration is also required to be given to any adverse impact on community confidence that may result from the use or conduct of a source or information obtained from that source.
- 8.6 Additionally, the authorising officer should make an assessment of any risk to a source in carrying out the conduct in the proposed authorisation.
- 8.7 Authorisation for the use of a CHIS must be given in writing. Only the Chief Executive or in his/her absence the person who is formally nominated to act as the Chief Executive may authorise the use of a juvenile or vulnerable CHIS.
- 8.8 Ideally the authorising officers should not be responsible for authorising their own activities e.g. those in which they themselves are to act as a source or in tasking a source. However it is recognised that this will not always be possible especially in the case of small departments. Authorisations must be approved by a Magistrate, see paragraph 7.5. The Solicitor employed by the Council will arrange the appointment before the Magistrate(s) and explain the procedure to the Authorising Officer. The Solicitor employed by the Council and the Authorising Officer will be required to attend before the Magistrate(s) to seek the Magistrate's approval to the authorisation.
- 8.9 An application for authorisation for the use or conduct of a source will be made on the appropriate form as set out at **Appendix CHIS/1** and must record:
- Details of the purpose for which the source will be tasked or deployed.
 - The reasons why the authorisation is necessary in the particular case and on the grounds on which authorisation is sought (e.g. for the purpose of preventing or detecting crime or disorder).
 - Where a specific investigation or operation is involved details of that investigation or operation.
 - Details of what the source would be tasked to do.
 - Details of potential collateral intrusion and why the intrusion is justified.
 - Details of any confidential material that might be obtained as a consequence of the authorisation.
 - The reasons why the authorisation is considered proportionate to what it seeks to achieve.
 - The level of authorisation required.
 - A subsequent record of whether authorisation was given or refused by whom and the time and date.

8.10 **Duration of Authorisations**

A written authorisation, unless renewed, will cease to have effect at the end of a period of twelve months beginning with the day on which it took effect except in the case of a juvenile CHIS which has a duration of one month. Oral authorisations will, unless renewed, last 72 hours.

8.11 Renewals

As with authorisations for directed surveillance authorisations for the conduct and use of covert human intelligence sources can be renewed, the same criteria applying. However before an Authorising Officer renews an authorisation, he must be satisfied that a review has been carried out of the use of a CHIS and that the results of the review have been considered. Applications for renewal must be made on the appropriate form as set out at **Appendix CHIS/3** and submitted to the authorising officer. However an application for renewal should not be made until shortly before the authorisation period is coming to an end.

8.12 An authorisation may be renewed more than once – provided it continues to meet the criteria for authorisation.

8.13 When covert human intelligence source authorisation requires renewal, the renewal must be approved by a magistrates' court in the same manner as an initial authorisation

8.13 Reviews

Regular reviews of authorisations should be undertaken. The results of the review should be recorded on **Appendix CHIS/2** and a copy filed on the central record of authorisations. If the surveillance provides access to confidential information or involves collateral intrusion frequent reviews will be required. The authorising officer should determine how often a review should take place.

8.14 Before an authorising officer renews an authorisation he must be satisfied that a review has been carried out of:

- The use made of the source during the period authorised
- The tasks given to the source
- The information obtained from the use or conduct of the source

8.15 If the authorising officer is satisfied that the criteria necessary for the initial authorisation continue to be met, he may renew it in writing as required. When covert human intelligence source authorisation requires renewal, the renewal must be approved by a magistrates' court in the same manner as an initial authorisation

8.16 Cancellations

The officer who granted or renewed the authorisation **MUST** cancel it if he/she is satisfied that

- the use or conduct of the source no longer satisfies the criteria for authorisation, or
- that the arrangements for the source's case no longer exist

8.17 Requests for cancellation will be made on the appropriate form as set out at **Appendix CHIS/4** and submitted to the authorising officer for authorisation of the

cancellation. All CHIS cancellations must include directions for the management and storage of any surveillance product.

8.18 Management Responsibility

The day to day contact between the Council and the source is to be conducted by the handler, who will usually be an officer below the rank of the authorising officer. No vulnerable person or young person under the age of 18 should be used as a source.

8.19 Security and Welfare

Account must be taken of the security and welfare of the source. The authorising officer prior to granting authorisation should ensure that an assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the target know the role of the

8.20 Confidential Material

Where the likely consequence of the directed surveillance or conduct of a source would be for any person to acquire knowledge of confidential material the deployment of a source should be subject to special authorisation. In these cases the proposed course of conduct must be referred to the Head of Paid Service or (in his absence) a Director for a decision as to whether authorisation may be granted.

8.21 Monitoring of personal information online

The study of an individual's on-line presence may engage privacy considerations requiring RIPA authorisation. The attached annex gives guidance on the monitoring of information online such as social media

9.0 MAINTENANCE OF RECORDS

9.1 Each Service shall keep in a dedicated place

- a record of all authorisations sought
- a record of authorisations granted and refused
- applications for the granting, renewal and cancellation of authorisations

9.2 The records will be confidential and will be retained for a period of 3 years from the ending of the authorisation.

9.3 Each authorising officer shall send original copies of all applications/authorisations, reviews, renewals and cancellations to the RIPA Co-ordinating Officer when drafted who will maintain a central record of all authorisations. The report will include details of the level of compliance with the requirements for authorisation.

9.4 Authorising officers will ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities in the handling and storage of material.

9.5 Where material is obtained by surveillance which is wholly unrelated to a criminal or other investigation or to the person subject of the surveillance and no reason to believe it will be relevant to future civil or criminal proceedings it should be destroyed

immediately. The decision to retain or destroy material will be taken by the relevant authorising officer.

10.0 AWARENESS OF THE CONTENTS OF THE ACT AND TRAINING

It shall be the responsibility of each Service Manager or other Authorised Officer to ensure that all staff involved or likely to be involved in investigations receive a copy of the training document, and are aware of the requirements and implications of the Act. It shall be the responsibility of the Senior Responsible Officer with the assistance of the RIPA Co-ordinating Officer to ensure that all relevant officers have received appropriate training and are aware of the requirements and implications of the Act.

11.0 CODES OF PRACTICE

A copy of each Code of Practice shall be kept in the reception area and be available to members of the public during usual working hours.

12.0 SENIOR RESPONSIBLE OFFICER AND RIPA CO-ORDINATING OFFICER

The Monitoring Officer is the Senior Responsible Officer for the Council whose role is:

- (i) to be responsible for RIPA training throughout the Council;
- (ii) to ensure that all authorising officers are of an appropriate standard; and
- (iii) to be responsible for heightening RIPA awareness throughout the Council.

The Senior Responsible Officer will nominate a Solicitor employed by the Council as the RIPA Co-ordinating Officer for the Council whose role is:

- (i) to collate all original applications/authorisations, reviews, renewals and cancellations;
- (ii) to keep the Central Record of Authorisations; and
- (iii) to notify the Leader of the Council of the receipt of authorisations from Authorising Officers.

13.0 MEMBER INVOLVEMENT

Members of the Community Wellbeing PDG should review this policy annually to ensure that it remains fit for purpose. Cabinet will consider reports from the OSC. The Cabinet should also consider reports on the use of the powers under the Act on a regular basis which shall be at least every year to ensure that it is being used consistently with this policy. Members of the Council will not however be involved in making decisions on specific authorisations.

Inventory of Surveillance Equipment held by MDCC

None as at 1 August 2019

Standard Operating Procedure for use of Surveillance Equipment

1. The Council operates the surveillance equipment (Equipment) as set out in the Inventory.
2. The Equipment should be stored, when not in use, in a locked cabinet under the control of the Senior Responsible Officer .
3. Any Officer of the Council considering using the Equipment for covert surveillance in a public place must make a written request to the Senior Responsible Officer or the RIPA Co-Ordinating Officer who will consider and decide whether the proposed use of the Equipment is appropriate bearing in mind the provisions of RIPA and the associated codes of practice.
4. Any Officer who uses the Equipment to record digital images may only view such images once captured and shall not download them on to a computer or other electronic storage facility unless this is first agreed by the Senior Responsible Officer and/or the RIPA Co-ordinating Officer.

Mid Devon District Council

Annex 1 to the Council's RIPA Policy

Open Source Internet Research and RIPA

Background

The internet enables access to a vast amount of information which can be useful to the Council in carrying out its statutory functions as well as engaging with the public.

Open Source Internet Research (OSIR) is the name given to viewing, collecting processing and analysing publicly available personal information stored on the internet including on Social Media. Social Media in this Annex means social networking websites such as Twitter, Facebook, YouTube, content communities and blogs.

This Annex to the Council's RIPA Policy covers the use of OSIR in investigations. Advice should be taken from HR should an investigation involve a member of staff. Where officers are carrying out OSIR they must be aware of the Council's RIPA Policy and the information contained in this annex.

Using OSIR raises the issue of whether RIPA authorisation must be obtained. This policy indicates when RIPA authorisation should be obtained. If RIPA authorisation is required the Council's RIPA policy must be complied with.

Investigatory techniques governed by RIPA

RIPA regulates the use of covert investigative techniques such as directed surveillance and CHIS, which are described in more detail in the Council's RIPA policy. RIPA requires that the use of these techniques must be authorised and judicial approved. The Council's RIPA policy sets out the process to obtain such authorisation and judicial approval.

Categories of using OSIR

This Annex focuses on four broad categories of OSIR to give an indication when RIPA authorisation is required.

Category 1

Category 1 is viewing publicly available postings or websites where the person viewing does not have to register a profile answer a question or enter correspondence in order to view e.g. a trader's website. There must be a low expectation of privacy and no RIPA authorisation would normally be required to view or record these pages.

However, repeated visits over time which amount to monitoring an individual's on line presence will require RIPA authorisation. How a person runs his/her business can be private information even if they do so in the public domain. No monitoring of a person's on line presence can take place without RIPA authorisation. The exception to this is where prior notification is given to the person that the Council is monitoring that person's on line presence. This would then be overt monitoring and would not require RIPA authorisation.

All visits to such websites for the purposes of any investigations must be recorded and be available for inspection by the Senior Responsible Officer and/or the Co-ordinating Officer-see Part 12 of the RIPA Policy for more details about these roles.

Guidance approved by the Senior Responsible Officer on record keeping of viewings will be distributed by the Co-ordinating Officer and must be adhered to. Using test purchases in an investigation does not necessarily trigger the need for RIPA authorisation but in each case advice must be sought beforehand from the Co-ordinating Officer

Category 2

Category 2 is viewing postings on social networks where the viewer has to register a profile but there is not otherwise a restriction on access. This would include Facebook where there is no need to be accepted as a "friend" to view. E.g. a trader has a "shop window" on Facebook advertising business and products

There are differences between this and Category 1. The person who posts information or runs such a website may reasonably expect viewers to work within the terms and conditions of the website. Viewings using a fictitious

identity or “covert account” require RIPA authorisation. No such viewings may take place without RIPA authorisation.

Viewing conducted in an overt manner do not require RIPA authorisation. Viewings can be conducted in an overt manner via an account profile which uses the officer’s correct name and email address (which should be a middevon.gov.uk).

All viewings for investigations regardless of whether RIPA authorised or not will need to be recorded and available for inspection by the Senior Responsible Officer and/or the Co-ordinating Officer. Guidance approved by the Senior Responsible Officer on record keeping of viewings will be distributed by the Co-ordinating Officer and must be adhered to.

Category 3

Category 3 is viewing postings on social networks which require a “friend” or similar status to view. Viewings using a covert account or fictitious identity will require RIPA authorisation. No such viewings may take place without RIPA authorisation.

Viewing conducted by using the officer’s correct name and email address (which should be a middevon.gov.uk) to acquire “friend status” may still require a RIPA authorisation. It may be that such a status is given by default on the part of the person posting or website owner. Officers will need to be sure that their access is being granted as a representative of the Council.

If officers are not sure that access is being granted to the officer as a representative of the Council then RIPA authorisation must be obtained before such viewings take place.

All viewings for investigations regardless of whether RIPA authorised or not will need to be recorded and available for inspection by the Senior Responsible Officer and/or the Co-ordinating Officer. Guidance approved by the Senior Responsible Officer on record keeping of viewings will be distributed by the Co-ordinating Officer and must be adhered to.

Category 4

Category 4 is the use of sophisticated OSIR tools and techniques including active search, reverse engineering and/or tools or filters etc to obtain information on an individual on the wider web. The use of such tools is likely to involve monitoring an individual and RIPA authorisation must be obtained before use

Covert Facebook accounts and similar covert social media accounts

Use of such covert accounts requires RIPA authorisation. Even with RIPA authorisation use of such covert accounts may be judged to be unlawful because the companies' terms and conditions do not allow such covert accounts. RIPA authorisation is not in itself sufficient to permit in law breaching a company's terms and conditions. Advice must be sought from the Co-ordinating Officer.

Procedures/instructions

Senior managers may issue instructions and procedure notes to provide further safeguards in using OSIR

This page is intentionally left blank