CITY OF CARDIFF COUNCIL
CYNGOR DINAS CAERDYDD

CABINET MEETING:21 JANUARY 2016

CCTV BODY WORN CAMERA POLICY AND PILOT DEPLOYMENT

REPORT OF CORPORATE DIRECTOR RESOURCES

AGENDA ITEM: 6

PORTFOLIO: CORPORATE SERVICES AND PERFORMANCE (COUNCILLOR GRAHAM HINCHEY)

Reason for this Report

1. To approve the Council's policy for determining the use of personal body worn CCTV camera equipment together with a pilot deployment.

Background

2. The development of body worn camera equipment has accelerated with many organisations across the UK and wider now implementing the equipment as part of their business practices.

3. Several service areas across the Council have requested to use CCTV body worn camera devices. It is important that as the Council changes the way it delivers services, whether this be through service improvement initiatives, or alternative delivery models, that a clear policy on the deployment and governance of body worn camera equipment, together with the decision making process is put in place. This will ensure the appropriate and lawful use of such technology throughout the Council.

4. The legislation, and the interaction of the legislation, which applies to body worn cameras is complex, and in order to manage the risks any deployment should be monitored closely. As a result the Council needs to put a policy and effective arrangements to assess, monitor and evaluate requests and deployments in place. This will ensure that the obligations and requirements of the Data Protection Act 1998, the Human Rights Act 1998, the Information Commissioner's CCTV Code of Practice and the Surveillance Commissioner's Code of Practice are all taken into account.

The Policy

5. The draft CCTV Body Worn Camera Council Wide Policy is attached (Appendix 1) and this Policy sets out the:

- strategic policy statement
- assessment process
- decision making process
- purpose for deploying Body Worn Cameras
- use and control of the devices
- staff training
- storage and retention of recordings
- access, viewing and disclosure of stored data
- audit arrangements
- review of the Policy

6. Appendix 1c to the Policy relates to the Privacy Impact Assessment. The Privacy Impact Assessment will be key to the decision making process as it assesses privacy i.e, the risks around the privacy of individuals in the collection, use and disclosure of information. This Assessment will also identify risks to individuals' privacy together with Data Protection compliance liabilities for the Council.

Pilot Arrangements

7. The draft Policy and the existing information governance arrangements have been used to assess and determine the pilot deployment in the Civil Parking Enforcement Team (Appendix 2)

8. The body worn cameras will assist in providing recorded visual and audio evidence of threats to safety in connection with any parking enforcement managed by the Council. They will be used for:

    - Staff safety and protection
    - Staff training and development

9. The operation of these cameras will be on a 'use when necessary' principle. This means that activation will only occur when there is a perceived act of aggression towards an officer and in order to ensure that these cameras are used appropriately and in accordance with the legislative requirements a review process has been built in. This will inform the overall evaluation of the deployment, including lessons learned to be fed into any future deployment requests.

10. Once the deployment of the cameras has been reviewed by both the service and the Improvement and Information Team further potential deployments will be assessed in line with the Policy. All deployments are approved by the Senior Information Risk Owner (SIRO), who has delegated authority under the Council's Scheme of Delegation to determine to manage and maintain compliance with the Data Protection Act 1998, and the Council's Data Protection policies and Privacy Impact Assessment requirements under the CCTV Code of Practice. It should be noted that the associated Privacy Impact Assessment and decision will be added to Appendix 1C of the CCTBV Body Worn Camera Policy in order to keep an accurate and up to date schedule of deployments.

11. The Improvement and Information Management Team will provide training for officers on the correct and appropriate use of the cameras and protocols prior to them being issued. The Civil Parking Enforcement Officers will also receive diversity training surrounding the appropriate use of the equipment prior to the devices being issued

12. The City Operations Directorate will be required to ensure that required provisions are in place to enable the Information Management Team and Internal Audit to undertake an audit of the use of the cameras, including spot checks, and to ensure that there are provisions in place to complete assessments and training on an annual basis.

13. The use of cameras will be for limited/specific purposes as defined within the Council's Policy and it should be noted that failure to use devices as outlined within specific parameters for which they are authorised would be classed as a breach of the Data Protection Principles and therefore a criminal offence.

Reasons for Recommendations

14. The Policy and decision making process will ensure that the risks associated with the use of the body worn cameras are managed, and that the pilot deployment will provide a level of evidence to inform a review of the implementation of the Policy.

Legal Implications

15. The legislation covering this area is as set out in the CCTV Body Worn Camera Council Wide Policy. Particular regard needs to be had to training, secure storage and appropriate processing of all recorded data to ensure compliance with the legislative requirements.

16. The Council has to satisfy its duties under the Equalities Act 2010 (including the specific Welsh public sector duties). Pursuant to these legal duties Councils must in making decisions have due regard to the need to:
(a) eliminate unlawful discrimination,
(b) advance equality of opportunity and
(c) foster good relations on the basis of protected characteristics

17. As such the decision on the recommendations in this report and will need to be made in the context of the Council's Equality Act public sector duties.

18. This will include undertaking an Equality Impact Assessment to ensure that the Council has understood the potential impacts of the decision in terms of equality so that it can ensure that it is making proportionate and rational decisions having due regard to the public sector equality duty.

Financial Implications

19. There are no financial implications arising directly from this policy. However, in implementing the policy the cost of the equipment and any other associated items will need to be funded from individual directorate budgets linked to the specific project. In respect of the pilot referred to in this report the costs will be funded from the Civil Parking Enforcement Account.

RECOMMENDATIONS

Cabinet is recommended to

1 approve the CCTV Body Worn Camera Council wide Policy (Appendix 1)

2 note the current delegation to the Council's Senior Information Risk Owner in relation to approvals for Body Worn cameras initiatives that accord with the Policy.

CHRISTINE SALTER
Corporate Director
15 January 2016

The following appendices are attached:

Appendix 1: City of Cardiff Council – CCTV Body Worn Camera Council Wide Policy
Appendix 2: Use of Body Cameras for Civil Enforcement Officers – Officer Decision Notice

Appendix 1

City of Cardiff Council

CCTV Body Worn Camera Council Wide Policy

Document Control

Organisation	City of Cardiff Council
Title	CCTV Body Worn Camera Council Wide Policy
Author	Information Security Board
Filename	
Owner	Senior Information Risk Owner
Subject	
Protective Marking	NOT PROTECTIVELY MARKED
Review date	Annually

Revision History

Revision Date	Revision	Previous Version	Description of Revision
1st December 2015	v 0.1		Initial document
9th December 2015	V0.2	V0.1	Amended to reflect the changes in approach to deliver a Council Wide Policy

City of Cardiff Council
CCTV Body Worn Camera Council Wide Policy

Introduction

This policy is a statement of the principles and assurances which govern the use of CCTV Body Camera units by the Council. It provides best practice advice for those involved in using CCTV Body Camera units and utilising the material recorded.

The Policy has been drawn up to govern the management of all operations of CCTV Body Worn Cameras within the Council which are subject to the provisions of the:

- Data Protection Act 1998
- ICO CCTV Code of Practice requirements
- Human Rights Act 1998
- Surveillance Commissioners' Code of Practice.

This policy will operate in conjunction with the Council wide CCTV Policy and Code of Practice

This policy will assist users of CCTV Body Camera units and users of information recorded on CCTV Body Camera unit to comply with their legal obligations under the Data Protection Act 1998 and where applicable, the Human Rights Act 1998 and the Freedom of Information Act 2000.

The adoption and implementation of this policy will also ensure

- ongoing compliance with any data protection good practice notes as may be released from time to time by the Information Commissioner's office
- that captured and retained images, and sounds, are of a suitable evidential quality
- confidence in the Council by those persons whose personal data may be captured, retained or shared

A number of appendices have been attached to this policy to assist in the deployment and usage of CCTV Body Camera units. These dependencies include links to corporate policies and processes which services will have to adhere to, and includes a copy of the Privacy Impact Assessment(s) completed where authorisation to use devices has been granted.

Strategic Policy Statement

The Council will not use CCTV Body Worn Cameras as “spy systems”. There will be no interest shown the deliberate monitoring of people going about their legitimate business.

CCTV Body Cameras will only be deployed in an overt fashion. The covert use of a CCTV Body Camera device will not be permitted.

All devices used by the Council must be encypted and procedures adopted by services to ensure the secure processing of personal data.

Assessment Process

All devices operated are subject to Privacy Impact Assessments in line with the CCTV Code of Practice to ensure they there are legitimate purposes for processing in line with the requirements of the Data Protection Act 1998 and Article 8 of the Human Rights Act 1998.

Decision Making Process

Each service of the Council who wish to use this technology will be required to have completed a Privacy Impact Assessment and the suitability of use will be considered and authorised by the Council’s Senior Information Risk Owner

Purpose for deploying Body Worn Cameras

The Council will deploy CCTV Body Camera units to assist in providing recorded visual and audio evidence for the following purposes:

- staff safety and protection,
- staff training and development

Use and Control of the Devices

Activation will only occur in cases where there is deemed to be a potential threat to officer safety.

Where a deployment of CCTV Body Camera unit is undertaken within the areas of staff safety and protection, it will be deployed in a 'use when necessary' mode. This means that the CCTV Body Camera in normal/default mode will be switched to off and the system will be switched on to 'record'

only when a staff member perceives aggression. The unit will remain in record mode until such time as the staff member considers that the threat is no longer perceived.

CCTV Body Camera units deployed for this purpose will enable partial records of staff movements and actions are obtained to:

- assist in the investigation of any allegation of assault or abuse where a staff member is either the alleged victim or alleged aggressor
- cater for any random or unexpected act of assault or abuse, staff, members of the public and investigating agencies can have a greater confidence in the fact that a recording has been made of the incident

The definition of Perceived Aggression in this context is:

- an individual threatening an Officer with a weapon, or other object
- an individual threatening an Officer with the intention of causing bodily harm
- an individual encroaching within an arms-length of an Officer (within their personal space)
- an individual making physical contact with an Officer

Any inappropriate use will be detected when the footage is later reviewed and any action that could give rise to concern will be fully investigated. All instances of when the CCTV Body Camera has been used for recording during a relevant activity or incidents will be logged by the officer who has used the camera and verified by a supervisor.

All staff using a CCTV Body Camera unit will visibly display a sign identifying their use of CCTV Body Camera equipment and as far as is practicable, inform members of the public who may be the subject of a recording that they are being recorded.

Staff Training and Development

Training will be provided by the Improvement and Information Team who will ensure that the appropriate staff are trained in the use of the device, their responsibilities, and the restrictions relating to the recording of activities and individuals. This training will take place in a controlled environment.

This training will be supplemented by specific training provided by accredited bodies such as City & Guilds based on the needs of the specific deployment.

All training will be recorded on the individual's HR file.

All staff using CCTV Body Cameras will be issued with specific managerial instructions relating to the use of CCTV Body Camera. This includes possible disciplinary consequences should they fail to use the device in an approved manner or should they tamper, or interfere, with recorded sound or images.

Storage and Retention of Recordings

For data protection purposes the Council will act as the Data Controller for any obtained or retained recorded material.

The Council will ensure that it complies with all necessary legislation and obligations and as such services authorised to use such technology will be required to have clear procedures established setting out how storage and retention of recordings will be handled.

All recorded material will be securely stored to ensure that at all times no unauthorised access to recorded material is allowed. All access to stored data will be recorded.

On a daily basis, or as and when an incident occurs, recorded material stored on a CCTV Body Camera will be transferred to a secure server on the Council system. Stored data must be retained in a manner that allows for a defined CCTV Body Camera unit's data to be separated from any other CCTV Body Camera unit's data and uniquely identified at all times.

Following the transfer of recorded material to a secure Council server, CCTV Body Cameras must be electronically cleansed to erase all stored data prior to any further usage.

Stored data or images will not be retained for longer than necessary. In some cases, especially where the data or images are to be used for legal purposes, it may be necessary to retain, data or images for longer than the normal retention period. Where it becomes apparent that stored data or images are no longer required to be retained, they should be deleted. The Council’s Corporate Retention Schedule will set out how long such information may be retained.

Access, Viewing and Disclosure of Stored Data

Access, viewing and disclosure of stored data will be controlled by the Council as Data Controller in adherence with this policy or any specific legislative requirement or obligation.

Access to stored data will be restricted to named and trained individuals/roles within the Council. Any unauthorised access must be reported immediately to the Parking Manager or the Data Protection Officer of the Council, who will take appropriate action.

All persons with access to stored data should be aware of the requirements of the Data Protection Principles as outlined in Appendix A of this Policy, which need to be followed when accessing stored data. All such persons should be aware that all access to stored data will be recorded and they must keep their password secure and not share it with anyone else.

Access to and disclosure of stored data to third parties will only be made in limited and prescribed circumstances. Details of those circumstances can be found in the framework code of practice for the sharing, disclosure or viewing of obtained or retained CCTV Body Camera data.

Where permitted, permanent copies of stored data will be provided on request in the form of a video. Video footage will be provided in line with the Council's Access to Information procedures.

Audit arrangements

An Audit Programme will be implemented by the Improvement and Information Team in conjunction with the Internal Audit Team. Services authorised to use CCTV Body Cameras will be expected to support these teams to ensure that spot checks are conducted and the use of devices assessed on an annual basis.

Review of the Policy

Due to the ongoing changes in legislation this Policy will be reviewed and updated annually.

Guide to Appendices

A number of appendices have been attached to this Policy to assist in the compliance with legislative requirements and to assist in the implementation of processes and procedures for the capture, retention, sharing and disclosure of obtained or retained data.

Appendix A

This provides a brief outline of the Data Protection Principles and the Councils Data Protection Policy.

Appendix B

This sets out the Councils Access to Information Procedures including the Data Protection Act Requests for Information Policy, Freedom of Information Requests and Environmental Information Regulations Requests procedures.

Appendix C

This provides the Privacy Impact Assessment(s) and the decision to approve their use. These will act as the schedule of deployments.

Appendix 1A

The Data Protection Principles

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless;

(a) at least one of the conditions in Schedule 2 is met; and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

2 Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

NB This is not a full explanation of the principles

More detailed information can be found on the Information Commissioner's website at www.ico.gov.uk.

Click to access the link to the Council's Data Protection Policy

Appendix 1B

Data Protection Act Requests for Information Policy

Document Control

Organisation	Cardiff Council
Title	Data Protection Act Requests for Information Policy
Author	Information Security Forum
Filename	
Owner	Senior Information Risk Owner
Subject	
Protective Marking	NOT PROTECTIVELY MARKED
Review date	Yearly

Revision History

Revision Date	Revision	Previous Version	Description of Revision
10th Oct 13	V 1.0		Cabinet approval of policy

Data Protection Act Requests for Information Policy

There are a number of different types of requests which can be submitted to the authority under the Data Protection Act which are outlined in this policy.

The procedures set out in this policy must be followed at all times when dealing with such requests.

Subject Access Requests (SAR's)

All Subject Access requests received by the Council must be forwarded onto the Improvement & Information team where they will be logged so that the Council has a clear record of the request and subsequent response issued.

Requests regarding more than one area of the authority will be managed by the Improvement & Information team with relevant officers contacted and asked to provide any information held (redacted where necessary). Requests relating to specific service areas will be passed onto the relevant area which will then be expected to manage such requests and respond directly to applicant. These requests are not quality assured by the Improvement & Information team.

The Council has developed letter templates which comply with our statutory obligations when dealing with Subject Access Requests under the Data Protection Act which must be used at all times.

Under the Data Protection Act 1998 a £10 fee is payable for anyone wishing to obtain their personal data. A request cannot be processed until the fee has been paid. The £10 fee, in line with the Council's Data Protection Policy & Procedure, will be waivered for current Council employees.

The 40 calendar days' response time commences from date of receipt of the fee. In the case of a request for an educational record, a fee up to a maximum of £50 depending on the number of documents held, may be required.

Any applicant must also supply the Council with proof of their identity. They must supply either a recent bank statement, or a utility bill, (within the last three months), and Photographic ID - i.e. Passport, Drivers Licence - this must be a clear photocopy.

It is best practice to send a copy of the Council's Subject Access Request form and guidance to anyone wishing to obtain their personal data to make it easier for individuals to advise of the specific data they wish to obtain and from which Council service(s). It is also best practice to pass this on if clarification or direction is required for such a request.

Council Guidance note on SAR Requests:
http://www.cardiff.gov.uk/ObjView.asp?Object_ID=22434&Language=&YYY=0

Cardiff Council's Subject Access Request form:

http://www.cardiff.gov.uk/ObjView.asp?Object_ID=22432&Language=&YYY=0

Subject Access Requests for CCTV Footage

Cardiff Council operates a CCTV system in partnership with South Wales Police. The system has 200 cameras throughout Cardiff and provides images which are used to manage the highway network throughout Cardiff and also for the prevention of crime and community safety.

Cardiff Council also operates cameras for providing evidence in criminal proceedings, providing evidence in civil proceedings or tribunals and for the prevention of crime.

There may be occasions when individuals request CCTV footage where they have been captured on cameras. This mainly occurs when a crime has taken place or for evidence to support an accident which has occurred.

All requests for CCTV footage must be processed as outlined in the Council's CCTV policy & Code of Practice.

The same identification and fee is required as per Subject Access Request provisions before processing any such request. If a request is submitted on behalf of someone else (i.e Insurance Company/Solicitor) the Council must ensure that consent has been supplied before information is passed onto anyone acting on behalf of the data subject.

Consent Form -

http://web1/corpqms/corporate%20general/Guidance%20Notes/FOI%20&%20EIR%20Letters/CCYV%20Templates/Consent%20Form.doc

Access to Health Records Act Requests

There may be occasions when relatives of the deceased request access to records which are classified as Health Records. Where this occurs requests should be dealt with under the Access to Health Records Act.

The person who requests such data must be the personal representative of the deceased and have a claim arising out of the person's death. A personal representative is the executor or administrator of the deceased person's estate.

Evidence must be provided to support that they are the executor of the deceased and the individual must also supply identification in the same way as the Subject Access Request provisions. This ensures that the Council can confirm their identity before providing any information.

In the main this type of request would be received by the Social Services area of the Council. It is important that a detailed record is kept of the request and how it has been dealt with. Copies of all correspondence (including emails) between the Council and the requestor must be kept together with any additional documentation.

Data Protection Act Section 29/35 Disclosure Requests

Sections' 29 and 35 of the Data Protection Act are exemptions within the non-disclosure provisions of the Data Protection Act. It allows the organisation to disclose information about a member of staff or citizen if requested by an outside organisation, which in normal circumstances may be a breach of the Data Protection Act.

Requests can come from organisations that can rely upon these exemptions because they have a crime prevention or law enforcement function and therefore have an appropriate purpose for requesting such information.

Main organisations that will request information under Sections 29 and 35 of the Data Protection Act are HMRC, the UK Border Agency, the Police, The Department for Work and Pensions or other local Authorities.

Any organisation requesting such information have to provide the Council with a completed Section 29/35 Disclosure form, (some organisations such as the Police who have their own form), otherwise they must complete the Council's Section 29 Disclosure request form.

The Council has a Section 29/35 Disclosure Request Form which can be forwarded onto any appropriate organsiation requesting information and a Guidance Note which should be followed when dealing with such requests.

Before information is released this must be authorised by the relevant Operational Manager or Chief Officer who must decide whether to release or not release personal information to the requestor. Officers should ensure that they refer to the Council's guidance on Section 29/35 Disclosure requests or contact the Improvement & Information team if they are unsure whether to disclose information.

Such requests should be managed within their relevant service areas unless they relate to a number of service areas in which case they should be immediately passed onto the Improvement and Information team who will be responsible for co-ordinating any such request on behalf of the authority.

A detailed record must be kept of the request and how it has been dealt with. Copies of all correspondence (including emails) between the Council and the requestor must be kept and also internal documentation.

Section 29/35 Disclosure Request Form -

http://web1.cardiff.gov.uk/corpgms/corporate%20general%2Fforms/Request%20for%20Disclosure%20of%20Personal%20Data%20Under%20Section%2029%20of%20DP.doc

Section 29/35 Disclosure Request Guidance Note - :

http://web1.cardiff.gov.uk/corpgms/corporate%20general%2Fguidance%20notes/Sec%2029%20%26%2035%20Requests%20for%20disclosure%20of%20personal%20information%20guidance.pdf?unique=1378459848

FOI/EIR Requests Policy & Procedure

Document Control

Organisation	Cardiff Council
Title	FOI?EIR Requests Policy & Procedure
Author	Information Security Forum
Filename	
Owner	Senior Information Risk Owner
Subject	
Protective Marking	NOT PROTECTIVELY MARKED
Review date	Yearly

Revision History

Revision Date	Revision	Previous Version	Description of Revision
[Date]	V 1.0		Initial document

Information Requests Policy

Introduction

The Freedom of Information Act 2000 is designed to promote greater openness and transparency throughout the public sector. Under the Act any person, has rights of access to recorded information held by the Council.

Requests for information can arrive in any part of the organisation by a number of means.

In responding to any request for information regard must be had to the potential impact of the Freedom of Information Act (FOI), the Environmental Information Regulations (EIR), the Data Protection Act (DPA) and the Councils policies on Access to Information.

Anyone responding to or handling a request for Information must take into account the policy agreed by the Executive on 4th November 2004 which states:

- The Council will consider that it is in the public interest to disclose information unless it can be clearly shown that it is in the public interest not to do so (e.g. because such disclosure would cause substantial harm or breach confidentiality). In particular the Council will not regard the following factors as reasons to withhold disclosure:

- that disclosure may reveal incompetence on the part of, or corruption within, or would cause embarrassment to the Council: and

- that information is too complicated for the applicant to understand, or that disclosure might misinform the public because it is incomplete.

Submitting a Request For Information

To request information from Cardiff Council, individuals should first check whether it is available through the publication scheme (in many cases it will be quicker to simply use the search facility on this website). If an applicant cannot find what they are looking for they should submit a formal request under the Act, giving as much detail as possible, using the contact details below:

Email: foi@cardiff.gov.uk

Post:
Information Request Officer,
Room 108,
County Hall,
Atlantic Wharf,
Cardiff Bay,
CF10 4UW

Submit an online request:
http://www.cardiff.gov.uk/content.asp?nav=2872,3252,4532,6313&parent_directory_id=2865&pagetype=&keyword

Processing of Requests for Information

There are three main options for processing requests:

- immediate release of routine and Publication Scheme Information,
- Business as Usual Response & Release by Service Area,
- official FOI/EIR Requests – Managed by the Improvement & Information Team and assisted by the relevant service area FOI Officers.

The Council has developed precedent letters which comply with our statutory obligations under the Freedom of Information Act and Environmental Information Regulations which must be used at all times.

Immediate Release

Information that is reasonably accessible to an applicant by other means is exempt from FOI. This includes information identified in the Council's Publication Scheme. Where a request can be fully satisfied by providing or referring to information identified in the Publication Scheme the only action required is:

- To provide, or refer the applicant to, the appropriate information in the manner identified in the Publication Scheme.

- There is no requirement either to record the request or the response for FOI purposes if the information is provided as above, unless the request specifically refers to FOI or EIR in which case it must be logged as an FOI request and Section 21 letter should be sent to record the transaction.

- Where information is exempted under Section 21 of the Act, a refusal notice under Section 17 does not have to be issued when the applicant is advised where and how the information may be obtained. Normal records of the communications should be kept so as to be able to satisfy the Information Commissioner that appropriate advice and assistance was given.

- Where information is available under the Publication scheme the response providing the information, or advising where it may be found, must be sent promptly and within five working days as a minimum. If the information needs to be viewed at the Council's premises, the Council must contact the individual within five working days to arrange an appointment convenient to both parties.

Business as Usual Response & Release by Service Area

Service Areas should handle the majority of routine requests for information that they receive in the normal way without logging them as FOI requests (unless the request specifically states FOI / EIR). This is the business as usual principle. There is no need to add any additional process or bureaucracy to the handling of simple requests.

Consideration should only be given to deal with such requests under FOI / EIR if the Council is considering not disclosing information, in which case FOI / EIR should be invoked to ensure lawful processes are followed if exempting information from disclosure.

If a request for information is submitted through complaints procedures specifically requesting information under FOI / EIR, dialogue should be opened up to deal with such requests through business as usual channels as part of the complaints procedure rather than added additional bureaucracy and dealing with the request under FOI / EIR.

However in such cases the applicant should be informed of this and advised that information disclosed specifically under FOI would be available to any other member of the public and that under the Council's duty to assist the customer it would be more beneficial to deal with the request without invoking FOI / EIR.

However care should be taken to ensure that information disclosed does not breach the Data Protection Act and other legislation in the same way as formal FOI / EIR requests.

If the applicant wishes to request information in relation to themselves this is exempt from FOIA/EIR. This type of request is known as a Subject Access Request and should be handled in line with the Data Protection Requests for Information Policy. These requests should be passed immediately to the Improvement and Information Team

Multi Service Area Requests – Managed by the Improvement & Information Team and assisted by the relevant service directorate officers.

Any such request for information will need to be logged and managed as a formal request where any of the following apply:

- Officers in receipt of the request anticipate for any reason that we may not, or cannot, answer the request in full.
- The request for information specifically mentions FOI or EIR.
- There is doubt about how to respond and advice from Improvement & Information about the implications of FOI, EIR or DPA is required.
- The effort expended in retrieving the information is estimated to incur costs (calculating staff time at £25 per hour) above the prescribed level (£450) i.e. more than 18 man hours work will be required to identify, locate and retrieve the information.
- The information cannot easily be provided in the form requested.

Decisions to exempt information from disclosure may be made primarily by Service Area FOI Officers and accompanied by required evidence to support the engagement of an exemption, but the ultimate decision on disclosure would be made by the Improvement & Information Operational Manager with the exception of the engagement of Section 36 exemption decisions which must be referred to the Council's qualified person.

Release and Refusal Process

The Improvement & Information team will be responsible for the release process and ensuring that any documents are correctly redacted as necessary in accordance with the decision made and that formal notices comply with legislative requirements concerning complaints and reviews – however the redacting process is the responsibility of officers within the relevant Service Area where the information had been obtained from.

The Improvement and Information team will quality assure all responses before they are

released. This is to ensure that exemptions are correctly applied and that redaction has been undertaking correctly.

The Improvement & Information team are responsible for ensuring consideration is given to the inclusion of a copyright warning either in the release letter or as a separate note if appropriate to the information disclosed.

The Improvement & Information team will also be responsible for issuing the appropriate notice in those cases where there is a refusal to confirm or deny holding information.

Yellow Paper Exempt Information

It is important to note that information exempt from disclosure at Council/Committees under the Local Government Regulations does not in itself exempt the material from disclosure under the FOI/EIR access regimes.

Such information must be supplied in respect of any requests submitted covering such information, and the Improvement & Information Team will seek the views of the Monitoring Officer when considering a request which covers such material.

Contracts

The Council is required under its Publication Scheme requirements, amended to reflect the requirements of the Protection of Freedoms Act 2012, to routinely publish dataset information, including information relating to contracts awarded by the Council.

All contracts should contain FOI/EIR clauses setting out the process of an information request being received, and third parties should be contacted and asked for their views on potential disclosure of information requested under FOI/EIR.

In line with the Ministry of Justice Guidance, authorities are strongly advised not to accept confidentiality clauses in procurement contracts that conflict with their obligations under the Freedom of Information Act and Protection of Freedoms Act.

Under the terms of the Freedom of Information Act the decision whether to withhold, or disclose the information, is ultimately a matter for the Council. This is regardless of whether the information was originally supplied by a third party. Te fact that a disclosure would be in breach of contract cannot be used as the primary factor in determining not to disclose the information under the Act (as there is no absolute exemption provided for this)"

Timescales

The 20 working day limit for processing requests means that all involved will have to work to very tight timescales. The timescales shown are a maximum and where one stage can be completed earlier, the next stage should be commenced immediately.

Compliance with requests will be reported in the Council's Quarterly Performance Reports, and failure to comply with requests within 20 working days can result in Enforcement Action being taken against the Council.

Reviews & Complaints

Cardiff Council operates an Internal Review procedure for FOI and EIR requests which aims to comply with the Section 45 FOIA Code of Practice and the Information Commissioners Office's Code of Practice on Internal Reviews. This procedure will be followed with any complaints regarding the handling of FOI/EIR requests

Responsibilities

The Council has a responsibility to make its recorded information available in accordance with the Data Protection Act. Corporate responsibility for ensuring compliance with this policy lies with the Senior Information Risk owner.

Day to day responsibility for co-ordinating the Council's Freedom of Information function lies with the Operational Manager, Improvement & Information.

All Members and Officers should familiarise themselves with this policy and the Freedom of Information Act and Environmental Information Regulations guidance which is available on the intranet.

Requests for personal information must be dealt with in line with the Council's Data Protection Requests for Information Policy.

Failure to comply with this policy could have serious consequences for the Council. It is important to seek advice if in doubt.

Publication Scheme

In addition to answering individual requests for information the Council has adopted, as required by the Freedom of Information Act, a legal publication scheme which sets out the type of information which it will make routinely make available. The Council has adopted the Information Commissioner's amended 2013 model scheme without modification which takes into account the requirements of publishing data sets in line with the Protection of Freedoms Act.

Related Policies

This policy should not be read in isolation. In particular this policy should be read in conjunction with the Council's:

a) Records Management Policy
b) Data Protection Policy & Procedure
c) Information Governance Strategy
d) Data Protection Requests for Information Policy
e) Information Management Strategy

Name of System: **Appendix 1C**
Responsible Officer:
If approved, anticipated go live date:

Privacy Impact Assessment Procedure

What is a PIA? A PIA helps assess privacy the risks around the privacy of individuals in the collection, use and disclosure of information and foresee any problems and assist in bringing forward solutions. A PIA will also identify risks to individuals' privacy together with DP compliance liabilities for the Council. This is important as there is a need to ensure that we protect the reputation of the Council and build public trust and confidence in what the Council proposes to do.

What are the risks of not carrying out a PIA?

The risks are:

- Need for re-design all or major parts of the system, which could be particularly costly if the risks are realised late in the development stage
- Collapse of the project or the completed system as a result of adverse publicity and/or withdrawal of support by key participating organisations
- Loss of credibility as the public perception is that the system does not protect their personal data adequately and safeguard their privacy
- Subsequent imposition of regulatory conditions as a response to public concerns, with the inevitable cost that entails
- Breach of privacy law, with the possibility of litigation and substantial financial penalties being issued against the Council.

When should a PIA be conducted?

A PIA must be completed at an early stage of a project, when: the project is being designed; you know what you want to do; you know how you want to do it; and you know who else is involved. However ideally it should be started before: decisions are set in stone; you have procured systems; you have signed contracts/agreements with any third parties

How should I do it?

If the PIA is being run as part of a project, every attempt should be made to integrate the PIA within that project. Privacy risks should not be considered in isolation from other types of risks – when determining priorities you need to weigh all risks against one another.

It is important to remember that a PIA is a process to ensure privacy risks are addressed throughout the lifecycle of the project – it is not about ticking boxes and producing documentation. Nevertheless, you also need

to have a record – usually in the form of a PIA Report - of the measures that were taken to address the privacy issues in the project. This is so that there is:

- accountability and transparency – the report is likely to be published under the Council's Freedom of Information Publication Scheme
- a basis for the post implementation review
- a basis for audit
- a record to be called up for future PIAs . PIA's can be re-used subject to appropriate review for subsequent substantially similar projects.

Who should do it?

Whoever is in a position to manage the risks and influence design decisions. For projects that is likely to be the project manager; for data sharing it is likely to be the Service Information Owner

The role of Improvement & Information Management

The Improvement & Information Management Team are corporately responsible for ensuring the Council's complies with privacy laws, including:

• The Data Protection Act,

• Privacy & Electronic Communication Regulations,

• Article 8 of the Human Rights Act,

• Freedom of Information Act & Environmental Information Regulations, and

• Links to Records Management requirements

The Improvement & Information Management Team will not approve the use of any new systems or processing of data without the completion of a Privacy Impact Assessment and formal record of the decision in respect of a project.

All Privacy Impact Assessments must be completed and returned to **DataProtection@cardiff.gov.uk**

What are the outcomes of an effective PIA?

The outcomes of an effective PIA will be:

- identification of a project's privacy impacts
- an appreciation of those impacts from the point of view of each group of stakeholders
- understanding of the acceptability of the project from those affected by it
- identification of ways to avoid negative impacts on privacy
- identification and assessment of less privacy-invasive alternatives
- where negative impacts on privacy are unavoidable, clarification of the business needs that justify them
- documented and published outcomes

What do I do next?

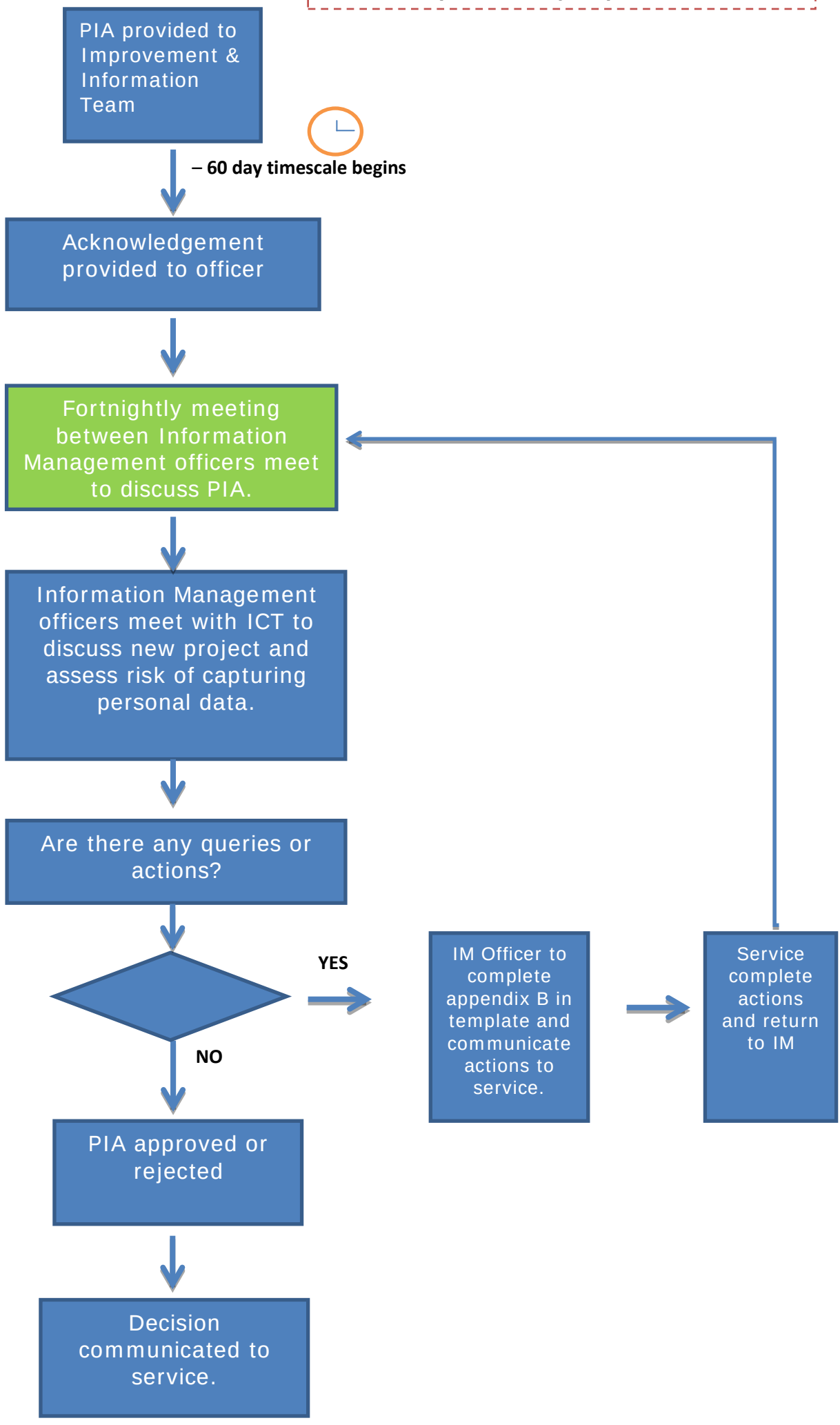
Consider Appendix A – Privacy impact assessment screening questions.
Complete Section 1 of the PIA (Appendix B).

Sections 2 and 4 are to be completed by the Information Management Team.

Section 3 is for ICT Security Team to complete.

A process map for Privacy Impact Assessments is overleaf. This will evidence the steps taken during the procedure.

Process Map for Privacy Impact Assessments



Privacy impact assessment screening questions (appendix a)

These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project/business changes develops if you need to.

Will the project / business change involve the collection of new information about individuals?

Will the project / business change compel individuals to provide information about themselves?

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Does the project / business change involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

The completion of the PIA will help the Improvement & Information Management Team address any relevant risks associated to your project/business change.

Section 1 of the PIA must be completed by the project team or service change lead, and submitted onto Improvement & Information Management Team to advise further.

The Improvement & Information Team need a minimum of 60 working days to consider section 1 of the PIA and may need further information in order to make a full determination of any privacy/data protection risks.

Please note, A PIA is not required where the service is simply contracting out with a data processor to process personal data within systems, but only in cases where the data processor will be conducting further services on behalf of the Council. You should consider the PIA in conjunction with the Council's Data Processor and Data Processing Guidance for staff.

Privacy impact assessment template (appendix b)

Section 1

Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the Council, to individuals and to other parties.

Please include the scope of the project and particular emphasise on how such data is intended to be processed. If a Project paper or Mandate already exists please also provide this as background.

If personal data is not involved in the Project/Business Change, a PIA is not required.

Using Technical systems or devices

If this Privacy Impact Assessment involves a technical/IT system, it is important to examine the ICT security risks involved in its application.

Please identify what system will be used and how it is managed and monitored.

Describe the information flows

Please advise where the data collected is obtained from. Does the project involve the use of existing personal data and will additional data be collected? Fully explain if how the data collated and processed at present.

To provide enough information to allow the Improvement & Information Team to consider this in full, please answer the following:

Please outline the types of personal/sensitive data which will be processed:

Who will have access to it?
[This includes both internally and externally. Describe any sharing arrangements and what the level of access is. It may help to produce a diagram to show the data flows.]

How will it be transmitted to third parties?
[If data is already been transmitted to third parties please describe how this is currently occurring and explain what if any agreements are already in place allowing for data to be transferred to such parties]

How will it be stored, kept up to date and disposed of when no longer required?
[This refers to all parties who have access to the information. How will the Council keep the information up to date, and ensure it is disposed of when no longer required. How will third parties if applicable also comply with this? Please detail the agreed retention details of such information.]

How are individuals whose data will be processed advised of the Council's potential processing of their data?
[This refers to data which the Council is the owner of. Does the Council have Fair Processing Notices/Disclaimers or information online which is provided to individuals' whose data may be processed in line with this project/business change advising of how the Council may process their information.]

Consultation requirements

Please provide a list of all individuals involved in the project and those that may be affected by it. At this stage you want to have as broad a list of groups as possible- this can be edited down at a later stage for more focused consultation.

Section 2 – (For Information Management to complete)

Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Any risks identified within this section should also be referenced on the service area Information Risk Return. Please consult with your service Information Asset Owner for further details.

Privacy issue	Risk to individuals	Preliminary assessment of Risk H/M/L

Identify privacy solutions

Describe the actions to be taken to reduce the risks, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems).

Risk	Solution(s)

Section 3 – (For ICT to complete)

ICT Security

If the project involves a new or existing technical system it is important to identify any risks to ICT security that may arise as a result of the implemented business change. Describe the risks to the organisation and to the individual whose data is being processed.

It is also important to indicate at this stage whether the solution requires sign off at ART. Please state **YES** or **NO** giving a full explanation for either answer.

Security Issue	Solution(s)	Preliminary Assessment of Risk H/M/L

Section 4 – (For Information Management to complete)

Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Action Monitoring

Please state the date on which the project was referred to the Information Management and ICT panel.

Who is responsible for the PIA actions?

Action to be taken	Date for completion of actions	Responsibility for action

Appendix C

Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?

Appendix 2

Use of Body Cameras for Civil Enforcement Officers

Background

Improvement & Information have been approached by the Network Management Team within City Management and provided with an initial Officer Decision report on the potential use of Body Cameras for Civil Enforcement Officers.

The contents of this report have been put together on the same basis as a report produced regarding the potential use of Body Cameras for Waste Enforcement Officers in August 2012.

In order to use such devices the Council has to be able to demonstrate that data processing would be valid under the Schedule 2 and Schedule 3 Conditions of the Data Protection Act and ensure that the use of the devices comply with the Information Commissioners Office CCTV Code of Practice and article 8 of the Human Rights Act.

The likely conditions fall under Schedule 3 are in bold in the following list:

- Explicit consent has been given by the data subject
- Necessary for the purpose of Employment rights/obligations
- **Necessary to protect the vital interest of the data subject or another person**
- Processing is carried our in the course of its legitimate activities
- Information contained in the personal data has been made public as a result of steps taken by the data subject
- Processing is necessary in connection with Public functions
- Necessary for compliance with any legal obligation
- Necessary for medical purposes

The officers have been asked to provide justification on how processing would meet any of the Schedule 3 conditions and as a result it has become apparent that the use of such devices would be for the Prevention and Detection of Crime and for the Health and Safety of the Civil Enforcement Officers. However if the Council was to use these as reasons for implementing this type of technology this would need to be backed up with sufficient evidence to demonstrate how the use would be proportionate.

The evidence provided by the Network Management Team and considered under the Data Protection Act – Schedule 3:

(i) Necessary to protect the vital interest of the data subject or another person

During the course of their duties, civil enforcement officers are presented on an almost daily basis with verbal abuse from motorists and the

general public. In most cases they accept this as a consequence of the role they carry out on behalf of the Council in enforcing parking contraventions. However, from time to time motorists can become angry and potentially violent and in such circumstance body worn CCTV cameras could be activated. It has been reported from other parties that the activation of these devices together with a verbal warning that recording is taking place has been shown to calm the situation down and protect the officer from attack.

Actual examples of serious physical assaults/ threats in the past four months include:

(a) On November 5th 2012 two CEOs were reporting a vehicle in May Street Cathays and had affixed the penalty charge notice to the vehicle. The owner arrived and immediately became aggressive, after which he leaned into the car and took out a metal bar/ torque wrench. He proceeded to chase one officer around the cars with the intention of causing grievous bodily harm. The Police were called and attended swiftly and apprehended the aggressor. This incident has been logged in the Council's dangerous occurrences records, and both officers took time off work to recover from the shock of the incident.

(b) On 11th November 2012 a CEO was physically assaulted in Charles Street and was struck to the ground, suffering a fractured elbow, cuts and bruises, and of course suffering shock afterwards. She is currently on extended sick leave and it is not known yet whether she will be able to return to work due to fear of repetition. The Police again attended rapidly and the aggressor was arrested and will face prosecution.

Although most incidents are accepted as "part of the job", a further 8 incidents have been deemed of sufficient gravity to be recorded on the corporate Health and Safety records over the period April 2011 to December 2012. In addition to these incidents there are many more lower level incidents that are not recorded and these occur on a daily basis.

Further information supplied:

For most of the time the camera would be switched off and it is only in cases of perceived aggression that the unit would be activated and recording would begin. The unit would be switched off again after the event to reduce unnecessary filming. The recordings should be linked to a potentially violent persons database (PACD) (justifying the recording) and stored securely on the Council's computer network and if not required would be deleted or over-written after say one month. Therefore, personal data would not be retained for longer than absolutely necessary.

Devices will be used to record incidents which can be used in Court proceedings. Additionally, it provides protection for the officers as it is a visible deterrent to any potential assailant, making a clear statement that their actions will be recorded, and records the actions of the officer, thereby reducing the

scope for false allegations. These issues are particularly relevant to officers required to work alone and uncorroborated in isolated areas. Whilst some areas of the County are covered by existing CCTV cameras, it should be stressed that not all of the areas of the County have such cameras, and also where there are cameras in some locations, the image recordings are not of a quality which would assist with any incidents/investigations.

Officers have also asked that such devices are equipped with the use of audio, and have agreed clear parameters in regard to perceived aggression as which point devices would either be switched on, or where practical the Enforcement Officer will advise the member of the public that they are going to switch on the device.

The definition of Perceived Aggression:

- An individual threatening an Officer with a weapon
- An individual threatening an Officer with the intention of causing bodily harm
- An individual encroaching within an arms length of an Officer (within their personal space)
- An individual making physical contact with an Officer

It should also be noted that Civil Enforcement Officers would use their training provided (City & Guilds) to ensure that situations are calmed to their best of their ability without the need to switch on the actual device.

Analysis

Upon looking into the justification provided a number of factors have been considered:

1. The use of CCTV has to be propionate to the purpose and there is enough evidence to back up how this could be justified. Based on the information provided this would in my view would be justified by the Information Commissioners Office.

2. The Information Commissioners' Office has recently provided guidance on the potential use of such devices which in line with the evidence supplied to us back up the potential use of such devices:

http://www.ico.org.uk/conference2013/~/media/documents/dpoc2013_documents/DPOC2013_Upholding_information_rights_in_the_world_of_surveillance.ashx

3. The devices could be potentially operated subject to a number of provisions which will ensure compliance with the Data Protection Principles:

Principle 1 (Fair Processing)

Clear and visible signs or audio announcements would be given to a member of the public that to inform them that devices would be switched on or being operated.

The devices would be clearly visible as demonstrated in appendix 1. There would also be notice given in the capital times, website and other media that officers were now equipped with such devices.

In most cases an Enforcement Officer would give a clear announcement that they intend to switch on the device, however it such be noted that in some cases it might not be possible for officers in certain situations to give a clear announcement before switching on the device.

Principle 5 (Retention of information)

Retention periods should reflect the Council's own purposes for recording images. Such images would be kept for no longer than 31 days in line with the Council's CCTV Policy and Code of Practice, and measures would be put in place to ensure permanent deletion through secure methods

Principle 6 (Individuals Rights)

The Council will need to ensure that it produces a clear Body Worn Cameras Policy to ensure that members of the public are aware of the reasons for processing and their rights to access.

Members of the public will have rights to request any recordings held under the subject access provisions of the Act, which would need to be in line with the Council's corporate Policy on access to information.

There may also be occasions with other parties (such as the Police) may request such information, and in any such cases the Council's Section 29/35 non disclosure provisions procedures must be followed.

Principle 7 (Security of Information)

The Council must ensure that such images are kept secure. Liaison will be required with ICT to ensure that the most appropriate secure systems are used for operation of such devices and that all images are downloaded directly onto the Council's secure network.

All Enforcement Officers will have to be provided with training (in line with the Council's requirements for under the CCTV Policy). Enforcement Officers will be provided with detailed Data Protection Training on the use of such devices, and a number of officers will need to be identified with the section to handle access requests for information (such officers would be required to obtain a Security Industry Licence).

Audit procedures will need to be put in place to ensure that devices are being used in line with the requirements set out in the Body Worn Camera Policy. An

annual review will be conducted with compliance with the system, however for the first 6 month period of the system being operated full audits will be conducted every 4-6 weeks between the Improvement & Information Team and Internal Audit to ensure devices are being correctly operated.

4. The key consideration for the Council is to ensure that:
- there is a pressing need to capture images of people in this way,
- give people appropriate information that such a system is in use,
- cameras should only be 'switched on' during incidents which warrant a recording being made.

5 The risk to the Council of using devices for recording audio as well as footage creates additional risks. The ICO has raised concerns about a trend for attaching microphones and sound recording equipment to cameras. The ICO has said that there are limited circumstances in which audio could be used, and given the particular purposes in this case I believe that this would also be justified, however Civil Enforcement Officers must inform members of the public of this, apart from where an incident occurs where the Civil Enforcement Officer does not feel that they are in a position/situation to be able to provide a clear message to the member of the public due to risk of harm being caused to themselves.

Findings/ Recommendation

The use of body warn cameras for Civil Enforcement Officers is in my view justified, subject to the provisions set out in this report being implemented:

1. A clear Policy being implemented to ensure compliance with the Data Protection Principles
2. Specific Data Protection training for the officers using the devices
3. A full audit programme is in place to ensure the devices are not misused

Evidence supplied backs up the potential use of such devices under the Schedule 2 and 3 Conditions of the Data Protection Act.

The ICO have previously advised that there may be safety issues in that by wearing these devices, officers may become targets for attack, and this also needs to be taken into consideration.

The Council does need to take extra care in consideration of any potential uses of such devices as the approval of the use of such devices could create an influx of officers who are more at risk of attack wishing to use such devices, the governance of which would be very difficult for the Council to control. Therefore it should be stressed that the fact that such officers lone work is not the key reason behind any decision to approve the use of such devices.

Recommendation

This recommendation was passed onto the Senior Information Risk Owner (Christine Salter) to make the final decision regarding the use of body worn cameras within the Network Management Team.

Decision

Based on advice contained within this report, I am content that the use of body worn cameras be supported within the Network management Team. However I would suggest that it reviewed after twelve months operation and I would wish to receive an update report at that stage in order to confirm outcomes were as expected.

Christine Salter (SIRO) 15 April 2013

Report Complied by: Dave Parsons, Information Officer

Agreed by: Vivienne Pearson, Operational Manager, Improvement & Information

Date: 12th April 2013

Agreed by SIRO: Yes

Appendices

Appendix 2.1 – Image of potential device*
Appendix 2.2 – Initial Officer Decision Report provided to Improvement & Information
Appendix 2.3 – Impact Assessment conducted into the potential use of such devices

* For clarity the images within Appendix 2.1 are different to that of the initial Officer Decision Report (Appendix 2.2) as the potential devices to be used changed from the date of the initial report.

Appendix 2.1

Image of device

Appendix 2.2

OFFICER DECISION : REPORT

ADDRESSED TO: Operational Manager (Network Management)

PREPARED BY OR ON BEHALF OF: Steve Carrel

The delegation to be exercised is in accordance with **4D1.1** of the Council Scheme of Delegations(Part 3 - Responsibility for Functions) and with paragraph 1.2 of the Service Area Business Plan

TITLE OF REPORT: Civil Enforcement Officers – Use of body worn CCTV cameras

PROPOSAL:

The recommended decision is:

1. That the principle of using body worn cameras for personal protection purposes only be approved, and
2. a process be commenced to acquire these devices via competitive tender.

The reason for the recommended decision is:

To offer personal protection to the civil enforcement officers when confronted with situations where the motorist is becoming aggressive and potential violence could arise.

1 STATEMENT

This report complies with the following general delegation in accordance with the Executive Scheme of Delegations.

The Corporate Director, Director, Operational Manager, shall be authorised:-

1.1 To make any decisions relating to any matter within their area of responsibility, provided always that the decision is:

a) within budget
b) in accordance with the Council's policy framework
c) in accordance with Council's Financial and Land Procedure Rules and Contracts Procedure Rules
d) in accordance with their Service Area Business Plan

e) not a matter specifically reserved for Full Council, a Committee of the Council, the Executive or a Statutory Officer.

1.2 To take appropriate action, which is necessary, to ensure the efficient, equitable and effective delivery of services.

1.3 To exercise the following Delegations: 4D1.1 – to make any decision within the Operational Manager's area of responsibility.

2 BACKGROUND

2.1 During the course of their duties, civil enforcement officers are presented on an almost daily basis with verbal abuse from motorists and the general public. In most cases they accept this as a consequence of the role they carry out on behalf of the Council in enforcing parking contraventions. However, from time to time motorists can become angry and potentially violent and in such circumstance body worn CCTV cameras could be activated. It has been reported from other parties that the activation of these devices together with a verbal warning that recording is taking place has been shown to calm the situation down and protect the officer from attack.

3 ISSUES

3.1 These cameras would be attached to the outside of the CEO's uniform and could either display the Council ID card of the officer or more likely the CCTV wording on the yellow background, as illustrated below. The one showing the CCTV wording might be preferable because it displays the potential for recording even while dormant and so could act as a deterrent without the need for activation. In the event of an aggressive incident the device would be activated by sliding the badge or lens cover downwards to reveal the lens and the message in yellow.

VideoBadge

- Protecting Staff
- Recording Evidence
- Managing Data

(these images are from a specific supplier's web-site and are used to illustrate the general product only)

3.2 For most of the time the camera would be switched off and it is only in cases of perceived aggression that the unit would be activated and recording would begin. The unit would be switched off again after the event to reduce unnecessary filming. The recordings would be stored securely on the Council's computer network and if not required would be deleted or over-written after say one month. Therefore, personal data would not be retained for longer than absolutely necessary.

3.3 Actual examples of serious physical assaults/ threats in the past four months include:

(a) On November 5th 2012 two CEOs were reporting a vehicle in May Street Cathays and had affixed the penalty charge notice to the vehicle. The owner arrived and immediately became aggressive, after which he leaned into the car and took out a metal bar/ torque wrench. He proceeded to chase one officer around the cars with the intention of causing grievous bodily harm. The Police were called and attended swiftly and apprehended the aggressor. This incident has been logged in the Council's dangerous occurrences records, and both officers took time off work to recover from the shock of the incident.

(b) On 11th November 2012 a CEO was physically assaulted in Charles Street and was struck to the ground, suffering a fractured elbow, cuts and bruises, and of course suffering shock afterwards. She is currently on extended sick leave and it is not known yet whether she will be able to return to work due to fear of repetition. The Police again attended rapidly and the aggressor was arrested and will face prosecution.

3.4 Although most incidents are accepted as "part of the job", a further 8 incidents have been deemed of sufficient gravity to be recorded on the corporate Health and Safety records over the period April 2011 to December 2012. In addition to these incidents there are many more lower level incidents that are not recorded and these occur on a daily basis.

3.5 It is the view of the managers of this area and the Health and Safety advisors that the use of these camera badges will assist in reducing serious verbal abuse and an escalation to violence and would show clearly to the officers that the Council values their safety. In such cases, the evidence collected by the device could be used by the Police in potential prosecutions and this would again send the appropriate messages to staff and the public.

3.6 If approved, setting up the devices would require liaison with ICT, the Data Protection Officer and possibly other services within the Council.

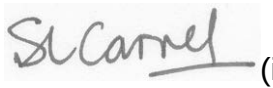
3.7 The CCTV camera units cost around £500 each, including the badge, software and charging equipment, but the tendering process would highlight whether cost reduction could be achieved by sourcing 50 units. Against this cost, it should be considered that the value of lost time in case (b) above will be significantly greater (current 3 months absence) than the cost of the CCTV unit which the CEO could have been carrying.

BACKGROUND PAPERS

The following are the background papers: None

I agree the report and submit it for formal approval of the recommendation/s

Name: S.L. Carrel

Signature:  (inserted electronically)

Designation: Team Leader (CPE)

Appendix 3

Cardiff Council Recording Devices Impact Assessment

Section 1.

1.1 CCTV Ownership & Operation

Who is the designated owner of the CCTV device(s)?

Steve Carrel, Network Management Team

Who are the designated operators of the device(s)?

Civil Enforcement Officers

1.2 CCTV Purpose

What is the proposed purpose for using CCTV? For example, the ICO CCTV Code of Practice identifies three main purposes for the use of CCTV which are Public Safety, Crime Prevention and National Security.

Prevention and Detection of Crime
Health & Safety of Civil Enforcement Officers

Do you need images of identifiable individuals, or could the system use other images not capable for identifying the individual? E.g. this is dependant on purpose; however it should be noted that traffic cameras monitoring the traffic flow would not need to produce identifiable images of individuals.

Yes, images need to be personally identifiable, which could be used in legal proceedings

1.3 Benefits

What are the benefits to be gained from the use of CCTV?

Devices will be used to record incidents which can be used in legal proceedings. Additionally, it provides protection for the officers as it is a visible deterrent to any potential assailant, making a clear statement that their actions will be recorded, and records the actions of the officer, thereby reducing the scope for false allegations. These issues are particularly relevant to officers required to work alone and uncorroborated in isolated areas. Whilst some areas of the County are covered by existing CCTV cameras, it should be stressed that not all of the areas of the County have such cameras, and also where there are cameras in some locations, the image recordings are not of a quality which would assist with any incidents/investigations.

Can CCTV realistically deliver these benefits?

Yes, as outlined in 1.3

Can less privacy intrusive solutions, e.g. improved lighting achieve the same benefits?

No, as outlined in 1.3 whilst there are existing cameras within the County in some areas, such devices are not fitted in every location of the County, and some of those devices operated by the Council are for traffic flow purposes and therefore do not provide adequate quality footage

1.4 Suitability

Will the particular equipment / system deliver the desired benefits now and remain suitable in the future?

Such devices would be annually reviewed to ensure continued suitability

What future demands may arise for the use of images and how will these be addressed?

These will be addressed through Corporate Procedures for handling subject access requests or requests under the non disclosure provisions of the Act, and will be outlined within a new Body Worn Camera Policy

1.5 Sustainability

Will/or does the particular equipment / system of work being considered deliver the desired benefits and remain suitable in the future? e.g., the cameras must be sited and the system must have the necessary technical specification to ensure the images are of the appropriate quality for each cameras stated purpose.

As outlined in 1.4

1.6 Mitigation

What are the views of those who are under surveillance? Has any consultation been sought on this?

Consultation is not required with members of the public on the use of such devices. In this case consultation has taken place between the Council Officers within Network Management and Improvement & Information, and also between the Council and Information Commissioners' Office

What could you do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed? For example, permanent and moveable cameras should be cited and image capture restricted to ensure they do not view areas that are not of interest and are not identified to be the subject of surveillance.

N/A

Do you have clear signage in place to let people know they are in an area where CCTV is in operation?

Such devices are clearly labelled as CCTV devices.
Members of the public will also be informed of the use of such devices through various communications (website, capital times)

Does the signage contain details of the organisation operating the system, the purpose for using CCTV and who to contact about the scheme?

The device will not be able to display this information, however officers will be aware of the reasons for recording and advise members of the public. Communications of the use of such devices will clearly stipulate this.

1.7 Legal

Is there a proper legal basis for the use of the system and is it operated in accordance with the Law? i.e. The Information Commissioners Office sets out a CCTV Code of Practice to ensure organisations comply with legal requirements of the Data Protection Act.

Yes, under Schedule 3 of the Data Protection Act - Necessary to protect the vital interest of the data subject or another person

Do the current devices capture the necessary quality of images that could be used for legal proceedings?

The intention is that such devices will capture images which could be used in legal proceedings

Section 2

2.1 Compliance with Privacy Laws

Note: The Data Protection Act (DPA) is relevant to any PIA, and a DPA compliance check should always be carried out.

2.2 Data Protection Act (DPA)

The template to use for the DPA compliance check is based on the one in Appendix 2 of the ICO's CCTV Code of Practice Revised Edition 2008 and can be found in Appendix A of this document.

A Data Protection compliance check has been carried out as part of this PIA, the details of which are in Appendix A. From this we have concluded (provide details)

2.3 Human Rights Act (Article 8) (HRA)

Note: In most cases HRA considerations will be covered by the other work on this PIA, including the DPA compliance check. If that is the case, you can simply record here that there are no special considerations that are not covered by other aspects of the PIA.

Section 3

3.1 Approval

Recommendation: Drawing on your analysis of the privacy risks, explain which option presents the best way forward. If significant risk remains, you should explain what the problem is and why the stakeholder consultation failed to resolve this.

Recommendations on the potential use of such devices will be outlined in a report to the Senior Information Risk Owner

Approval: Please record below who has approved the recommendation at 8.1 and the terms of that approval

Section 4

4.1 Review or audit

Note: Indicate below how and when an audit or review will be carried out.

Completed by:D.Parsons/A.Lane Improvement and Information Team
Date: 28/3/13