# RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

# DATA PROTECTION POLICY

**Date: 01.04.2018**

## 1. INTRODUCTION

1.1 Rhondda Cynon Taf County Borough Council needs to collect personal and sometimes sensitive information to deliver its services and to comply with the requirements of Laws and Regulations. In addition, the Council is also responsible for sharing information in accordance with requirements placed upon it.

1.2 No matter how it is collected, recorded and used, information must be dealt with properly to ensure compliance with General Data Protection Regulations (with effect from 25th May 2018).

1.3 Processing information in a lawful manner is extremely important to the Council and demonstrates clear accountability and transparency to our customers.

1.4 This Policy provides an overview of the Council's governance arrangements in respect of managing the information that it processes and it applies to all Workers. It includes organisational measures and individual responsibilities which aim to ensure that the Council complies with the General Data Protection Regulations and respects the rights of individuals.

## 2. LEGAL REQUIREMENTS

### General Data Protection Regulation (GDPR)

2.1 The General Data Protection Regulation 2016 (GDPR) replaces the Data Protection Act 1998 (DPA) (with effect from 25th May 2018).

2.2 The regulation governs how information about people (personal data) should be treated. It also gives rights to the individuals whose data is being processed and held. It applies to any data that relates to "an identified or an identifiable natural person (data subject)".

2.3 The GDPR is fully retrospective, in that it applies to information collected prior to the regulation coming into force.

2.4 The GDPR is enforced by the Information Commissioner. There are a number of tools available to the Information Commissioner for taking action to change the behaviour of organisations that process personal information where the law is broken. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve monetary penalties:

- Tier 1 - €10M or 2% of worldwide annual turnover for administrative errors e.g. failing to notify a breach when required to do so.

- Tier 2 - €20M or 4% of worldwide annual turnover for failing to comply with the principles or breaching data subject rights e.g. failing to keep personal information secure, failing to comply with a request for personal information.

## 3. SCOPE

3.1 This Policy applies to all employees, contractors, consultants, partners, suppliers, agents or anyone with access to personal data held by or on behalf of the Council.

3.2 The Policy also applies to personal data processed by Elected Members when representing the Council, for example as a member of a committee.

3.3 The Policy applies to all processing of personal data for which the Council is the Data Controller. This includes:

- Personal data processed by the Council.
- Personal data controlled by the Council but processed by a third party on the Council's behalf (for example private sector contractors).
- Personal data processed jointly by the Council and its partners (data controllers in common).

3.4 Data subjects may include, but are not limited to:

- Customers
- Clients
- Service users
- Citizen
- Current, past and prospective employees
- Others with whom the Council communicates

3.5 The Policy applies to all personal data regardless of the media in which it is held including electronic data, CCTV, video and sound recordings and data held in physical format (e.g. paper records).

## 4. LINKS TO OTHER POLICIES

4.1 A suite of supporting procedures, guidance documents, toolkits and frameworks underpin this Policy. These documents form the Council's Information Management Framework and help to demonstrate a commitment to accountability and transparency.

4.2 This policy may also be further supported by departmental procedures, guidance and information sharing protocols for specific areas of work.

## 5.0 GENERAL DATA PROTECTION REGULATION - PRINCIPLES

5.1 The GDPR contain 6 key principles and these effectively summarise the main responsibilities placed upon organisations. The following summarises the 6 principles and illustrates how the Council will aim to comply with each of them:

### 5.2 Principle (a) - Personal data shall be processed lawfully, fairly and in a transparent manner

In order to comply with this principle the Council will inform data subjects what we do with their personal data. This means that the Council will aim to:

- Review the purpose of our processing activities and establish an appropriate lawful basis for each activity.

- At the point that we collect personal data we will explain in a clear and accessible way:
    - What personal data we collect;
    - For what purposes;
    - Why we need it;
    - How we use it;
    - How we will protect the personal data;
    - To whom we may disclose it and why;
    - How data subjects can update their personal data that we hold; and
    - How long we intend to keep it

- Tailor this information for children, staff and other groups of people as appropriate.

- Publish this information in the form of 'Privacy Notices' and these will be made available on our website, and where appropriate in printed formats.
    - Privacy Notices will be reviewed regularly, and should significant changes occur data subjects will be informed.

- Where we process personal data to keep people informed about Council services, activities and events we will provide in each communication a simple way of opting out of further communications.

- Wherever consent is required to process personal information, the Council will aim to :
    - Make the request for consent prominent and separate from our terms and conditions.
    - Not use pre-ticked boxes or any other type of default consent.
    - Ask people to positively opt in and will provide clear instructions regarding withdrawal of consent.
    - Ensure that individuals can refuse to consent without detriment.
    - Specify the purpose for processing.

## 5.3 Principle (b) - Personal data shall be collected for specified, explicit and legitimate purposes

In order to comply with this principle the Council will verify that the processing is necessary for the relevant purpose, and ensure that it is satisfied that there is no other reasonable way to achieve that purpose.

## 5.4 Principle (c) - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

## 5.5 Principle (d) - Personal data shall be accurate and, where necessary, kept up to date

## 5.6 Principle (e) - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary

In order to comply with the three data quality principles above the Council will:

- Obtain and process personal data only to the extent that is necessary to perform its functions and deliver services i.e. personal data will be relevant to the stated purpose and adequate but not excessive.
- Ensure, as far as is practicable, that the information held is accurate and up-to-date.
- If personal data is found to be inaccurate, this will be remedied as soon as possible.
- Share personal information, such as contact details, within the Council where it is necessary to keep records accurate and up-to-date, and in order to provide individuals with a better service.
- Will retain personal data only for as long as required.
- Apply the Council's Retention & Disposal guidelines.
- Keep records only for as long as required in accordance with this policy.
- Dispose of personal information by means that protect the right of those individuals i.e. shredding, confidential waste, and secure electronic deletion.

## 5.7 Principle (f) - Personal data shall be processed in a manner that ensures appropriate security of the personal data

In order to comply with this principle the Council will take appropriate steps to safeguard all personal data it holds and minimise the risk of loss, wrongful access or improper use. This means that the Council will:

- Control access to personal data so that staff, contractors and other people working on Council business can only see such personal data as is necessary for them to fulfil their duties.
- Require all Council staff, and others who have access to personal data in the course of their work to complete basic data protection training, supplemented as appropriate by procedures and guidance relevant to their specific roles.
- Set and monitor compliance with security standards for the management of personal data as part of the Council's wider framework of information security policies and procedures.
- Provide appropriate tools for staff, contractors, and others to use and communicate personal data securely and when working away from the main

office environment when their duties require this, for instance through provision of secure virtual private network or encryption.

- Take all reasonable steps to ensure that all suppliers, contractors, agents and other external bodies and individuals who process personal data on behalf of the Council enter into a Data Processor Agreement and comply with auditable security controls to protect the data.

- Take all reasonable steps to ensure that information is not transferred outside the European Economic Area, without verifying that the organisation processing the personal data has provided adequate safeguards.

- Develop and maintain Information Sharing Agreements (in keeping with Welsh Government's Wales Accord on the Sharing of Personal Information framework) with partner organisations and other external bodies with whom we may need to share personal data to deliver shared services or joint projects to ensure proper governance, accountability and control over the use of such data.

- Make appropriate and timely arrangements to ensure the confidential destruction of personal data in all media and formats when it is no longer required for Council business.

## 6.0 INFORMATION RIGHTS

6.1 The GDPR provides certain rights to individuals. The Council is committed to ensuring individuals can freely exercise their rights and has procedures in place to ensure staff are aware of and can respond to requests of this nature. Below is a summary of those key rights:

**i. Right to access**

This allows the individual to ask the Council if it holds personal information about them, what it uses the information for and to be given a copy of that information.

**ii. Right to correct incorrect information (rectification)**

This allows the individual to ask the Council to have their personal information rectified if it is inaccurate or incomplete

**iii. Right to erasure**

This allows the individual to ask the Council to have their personal information deleted or removed if there is no compelling reason for its continued use. This is not an absolute right and only applies in certain (limited) circumstances.

**iv. Right to restrict the use of your information**

This gives the individual the right to ask the Council to block or stop using their personal information if its continued use causes them substantial and

unwarranted damage or distress. This is not an absolute right and only applies in certain limited circumstances.

**v. Right to portability**

This right allows the individual to ask the Council for an electronic copy of their personal information in a readable format so that they may provide it to another organisation or service provider. The right to portability applies in certain limited circumstances.

**vi. Right to object to the use of your information**

This right allows the individual to object to the Council processing their personal information:

- Where processing is based on legitimate interests of the performance of a task in the public interests / exercise of official authority
- For direct marketing purposes
- Profiling
- Research purposes

**vii. Rights in relation to automated decision making and profiling**

This right enables the individual (in some circumstances) to object to the Council making significant decisions about them where the decision is completely automated and there is no human involvement.

## 7. ROLES AND RESPONSIBILITIES

7.1 To ensure compliance with data protection legislation everyone from front line staff to senior managers must understand their role and responsibilities when managing personal data. This creates clear lines of leadership, accountability and governance, as well as promoting a corporate culture where personal information is valued and protected.

7.2 Specific roles, responsibilities and governance arrangements have been established in line with data protection legislation and wider Local Public Services Data Handling Guidelines.

Key roles/groups are as follows:

**i. Senior Information Risk Owner**

The Group Director, Corporate & Frontline Services is the Council's designated Senior Information Risk Owner (SIRO).

The SIRO is a key role within the Council and oversees the systems and processes in place to safeguard information assets and that any risk associated with information is appropriately managed.

The SIRO is a member of the Council's Senior Leadership Team and is supported by the Council's Data Protection Officer.

### ii. Data Protection Officer (Statutory Post)

The Council's Principal Information Management & Data Protection Officer is the designated DPO for the Council. The DPO provides interpretation, advice and support on complex information governance and information compliance issues.

The Council will ensure that it provides adequate resources to support the DPO in discharging its responsibilities in accordance with the GDPR obligations.

Operationally the DPO reports to the Head of ICT. However, arrangements are in place whereby the DPO also has a reporting line directly to the Group Director, Corporate & Frontline Services (SIRO) in order to ensure organisational independence and objectivity. The reporting lines of the DPO are illustrated in appendix II.

### iii. Information Management Board

The Information Management (IM) Board provides high level oversight of the Council's Information Management arrangements. It determines the long term information management plan for the Council, monitors progress against the plan and provides assurance that information risk is being properly assessed, controlled and mitigated.

The Board is chaired by the SIRO and permanent group members consist of:

- Group Director, Community & Children's Services
- Director – Public Health, Protection & Community Services
- Head of ICT
- Head of Legal – Corporate & Democratic Services
- Head of Organisational Development
- Head of Internal Audit & Procurement Delivery Programme
- Head of Transformation & Data Systems
- ICT Programme & Support Manager
- Principal Information Management & Data Protection Officer

### iv. Information Management Team

The team supports the delivery of the information management plan. It delivers awareness training, provides advice and guidance to all Council Services and is also responsible for independently investigating reported breaches of procedure.

The representatives are as follows:

- Head of ICT,
- ICT Programme & Support Manager
- Principal Information Management & Data Protection Officer

- Information Security Officer
- Information Management & Security Assistant

### v. Information Management Working Group

The group supports the delivery of the information management plan, and is responsible for operationally supporting, monitoring and learning from information security incident investigations and raising awareness of Information Management and Data Protection within their Service Group.

The group is attended by key service representatives whose role is to provide a first point of contact for staff and managers for advice and information on information management related issues including data protection, information security and information sharing within their service.

### vi. Information Asset Owners (IAO)

The role of the IAO is assigned to Officers who have ultimate ownership and accountability of information systems and assets held within their service area. This is typically identified at a Head of service level.

IAO's have responsibility for making sure that information systems and assets are handled and managed appropriately. This means making sure that personal information is properly protected, and where personal information is shared, that proper confidentiality, integrity and safeguards apply.

IAO's are responsible for ensuring that their staff process personal data in compliance with the 6 principles of the GDPR (as set out earlier in Section 5 of the report).

### vii. All Data Users

Almost every member of staff within the Council handles and manages personal information as part of their day-to-day role and as such they all have an important role in effectively managing information throughout its lifecycle i.e. from the time it's created, to the time it's no longer needed and disposed of.

Individual Responsibilities:

- All data users must comply with this Policy. Failure to comply may result in disciplinary action which could lead to dismissal.

- Take part in relevant training and awareness provided by the Council to support compliance.

- Take all necessary steps to ensure that no breaches of personal data result from their actions.

- Report all suspected information security breaches promptly so that appropriate action can be taken to minimise harm.

## 8. RECORDS OF PROCESSING ACTIVITY

8.1 The GDPR contains explicit provisions regarding the need for organisations to document their processing activities. In order to discharge this key responsibility, the Council has in place an Information Asset Register (IAR). The IAR documents the following for each processing activity:

- purpose for processing
- legal basis for processing
- arrangements in respect of information sharing (with both internal and external partners)
- retention requirements
- information required for privacy notices;
- records of consent
- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessment reports
- Records of personal data breaches.

8.2 Each IAR will be subjected to regular review.

## 9. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

9.1 The Council will apply 'privacy by design' principles when developing and managing information systems and processes involving personal data.

9.2 Specifically the Council will:

- Undertake proportionate DPIA's to identify and mitigate data protection risks at an early stage of a project where new technology is being deployed or the processing is likely to result in a high risk to the rights and freedoms of individuals.

- Collect, disclose and retain the minimum personal data for the minimum time *necessary* for the purpose (i.e. adopt data minimisation)

- Anonymise personal data wherever necessary and appropriate, for instance when using it for statistical purposes

## 10. BREACHES OF PERSONAL DATA

10.1 The GDPR introduces a duty on all organisations to report certain types of personal data breaches to the relevant supervisory authority (Information Commissioner). This must be done within 72 hours of becoming aware of the breach, where feasible.

10.2 If the breach is likely to result in a high risk of adversely affecting individual's rights and freedoms, the organisation must also inform those individuals without undue delay.

10.3 The Council has robust breach detection, reporting and investigation procedures in place that aim to ensure that:

- Data breach events are detected, reported, categorised and monitored consistently.
- Incidents are assessed and responded to appropriately.
- Action is taken to reduce the impact of disclosure.
- Mitigation improvements are put in place to prevent recurrence.
- Serious breaches will be reported to the Information Commissioner.
- Lessons learnt are communicated and actions to help prevent future incidents are agreed and monitored.

## 11. DATA PROTECTIONS COMPLAINTS

11.1 The Council is committed to dealing effectively with any complaints or concerns individuals may have about the way in which the Council processes personal information. Any complaints about the Council's processing of personal data and rights under the Regulation will be dealt with in accordance with this Policy and the Council's Complaints & Concerns Policy.

11.2 Data protection complaints may be addressed directly to the Council's Information Management Team (email/address below) or may be submitted by any of the means highlighted in the Council's Complaints & Concerns Policy:

RCTCBC
FAO: Information Management Team
Bronwydd House
PORTH
RCT
CF39 9DL
e-mail: information.management@rctcbc.gov.uk

11.3 The GDPR does not set out a specific complaints regime for data protection issues. However individuals do have a right to request that the Information Commissioner make an assessment of compliance of particular circumstances with the GDPR.

The Information Commissioner's Office
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF

www.ico.org.uk Telephone: 03031231113 or 01625545745

11.4 The Council will respond promptly and fully to any request for information about data protection compliance made by the Information Commissioner.

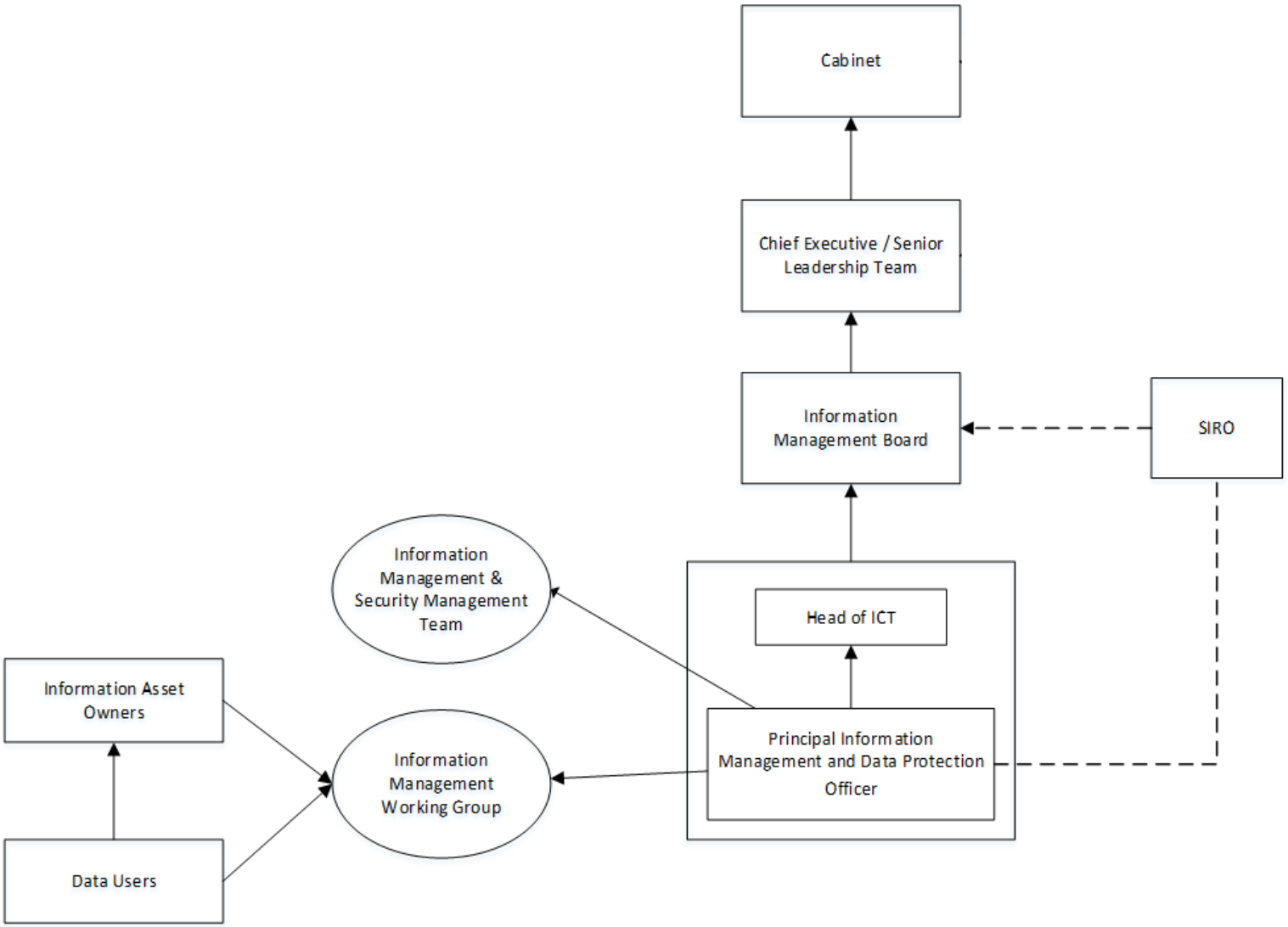
**Appendix I**

**DEFINITIONS**

| | |
|---|---|
| **GDPR** | General Data Protection Regulation 2016 |
| **DPA** | Data Protection Act 1998 |
| **Personal data** | Personal data is defined as - any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| **Special categories of data** | Formerly known as sensitive data, the categories are as follows:<br>• racial or ethnic origin,<br>• political opinions,<br>• religious or philosophical beliefs,<br>• trade union membership<br>• genetic data,<br>• biometric data for the purpose of uniquely identifying a natural person,<br>• data concerning health<br>• data concerning a natural person's sex life or sexual orientation |
| **Data Subject** | A Data Subject is a living individual to whom the personal data relates. Within the Council this could be a member of the public or an employee. |
| **Data Controller** | A Data Controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. |
| **Joint Data Controller** | The term jointly is used where two or more persons / organisations act together to decide the purpose and manner of any data processing |
| **Data Controller in common** | The term applies where two or more persons / organisations share a pool of personal data that they process independently of each other. |
| **Data Processor** | A Data Processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. |

| | |
|---|---|
| **Processing** | The definition of 'processing' is very wide and covers virtually any action associated with personal data including (but not limited to) obtaining, recording, viewing, storing, amending, sharing, viewing, disclosure, sharing and destruction of the data. |
| **Data User** | The term data user applies to any member of staff, member, contractor or third party who processes personal information held by, or on behalf of the Council. |
| **Information Commissioner** | The Crown appointed person (and department) responsible for the implementation and the policing of the Data Protection Act 1998 and the Freedom of Information Act 2000. He has the authority to both investigate and prosecute on behalf of any individual who believes that their Personal Data is not being handled in accordance with the legislation. |
| **ICO** | Information Commissioner's Office |

**Appendix II**


Cabinet
Chief Executive / Senior Leadership Team
Information Management Board
SIRO
Information Management & Security Management Team
Head of ICT
Information Asset Owners
Information Management Working Group
Principal Information Management and Data Protection Officer
Data Users