RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

DATA PROTECTION POLICY V.2.2

WEF: 17.01.2024

Contents

1. INTRODUCTION

1.1 Rhondda Cynon Taf County Borough Council needs to collect personal data 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 personal data is collected, recorded and used, the data must be dealt with properly to ensure compliance with Data Protection legislation.

1.3 Processing personal data in a lawful manner is extremely important to the Council and demonstrates clear accountability and transparency to our citizens, service users and customers.

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

2. LEGAL REQUIREMENTS

UK General Data Protection Regulation

2.1 The UK General Data Protection Regulation is UK law that came into effect on the 1st January 2021.

2.2 The GDPR sets out the key principles, rights and obligations for the processing of personal data in the UK, except for law enforcement and intelligence agencies (this is covered in the DPA).

Data Protection Act 2018

2.3 The Data Protection Act 2018 (DPA) came into effect on the 25th May 2018. It updates and replaces the Data Protection Act 1998. It was amended on the 1st January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

2.4 The DPA sits alongside and supplements the UK GDPR. It also sets out separate data protection rules for law enforcement authorities, extends data protection to other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.

Enforcement Action

2.5 The GDPR and DPA is regulated by the Information Commissioner / Information Commissioners Office (ICO).

2.6 The ICO offers advice and guidance, promotes good practice, monitors breach reports, conducts audits and advisory visits, considers complaints, monitors compliance and takes enforcement action where appropriate.

2.7 The ICO has a number of powers to take action against an organisation that has breached the GDPR or DPA. They include issuing;

- An assessment notice
- A warning
- An enforcement notice
- A penalty notices

2.8 For serious breaches of the data protection principles, the ICO has the power to issue fines of up to £17.5 million or 4% of global annual turnover, whichever is higher.

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 (joint data controllers).

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

- Customers
- Clients
- Service users
- Citizens
- 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 GDPR PRINCIPLES

5.1 Article 5 of the GDPR sets out seven key principles which lie at the heart of the UK's general data protection regime.

5.2 Article 5(1) requires that personal data shall be:

> "(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
>
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

5.3 Article 5(2) requires that:

> "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

6.0 COMPLYING WITH THE PRINCIPLES

6.1 The following sets out how the Council will aim to comply with each of the principles.

6.2 Article 5(1)(a) – Lawfulness, fairness and transparency

Lawfulness

6.3 The Council will identify an appropriate lawful basis (or bases) for processing personal and special category data.

6.4 If criminal offence data is processed, we will determine the condition for processing the data, or identify our official authority for processing the data.

6.5 The lawful basis (or bases) / condition for processing the data will be documented in the Council's Data Protection Register and reflected in the service privacy notices that are published on the Council's website.

6.6 Wherever consent is the lawful basis for processing the personal data, the Council will aim to:

- Make the request for consent prominent and separate from other terms and conditions.
- Not use pre-ticked boxes or any other type of default consent.
- Ask individuals to positively opt in.
- Provide clear instructions regarding the right to withdraw consent and how this may be exercised.
- Ensure that individuals can refuse to consent without detriment.

6.7 Transparency

6.8 The Council will be clear, open and honest with individuals about the processing of their personal data.

6.9 At the point personal data is collected we will explain/provide to individuals:

- The name and contact details of the Council
- Contact details of the Data Protection Officer
- The purpose for processing the data
- The lawful basis (or bases) for processing the data
- The legitimate interests for the processing (if applicable).
- The categories of personal data processed (if the personal data is not obtained from the individual it relates to).

- The source of the personal data (if the data is not obtained from the individual it relates to)
- Recipients or categories of recipients of the personal data
- Retention periods for the data
- The rights available to individuals in respect of the processing
- The right to withdraw consent (if applicable)
- The right to lodge a complaint with the ICO
- The details of the existence of automated decision-making, including profiling (if applicable)

6.10 We will do this in a concise, transparent, intelligible, easily accessible, way using clear and plain language.

6.11 The Council will tailor privacy information for children and other groups of individuals as appropriate.

6.12 We will publish privacy information in the form of 'Privacy Notices' and these will be made available on our website, and where appropriate in printed formats.

6.13 Privacy Notices will be reviewed regularly and should significant changes to the processing of personal data occur, individuals will be informed as appropriate.

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

6.15 Article 5(1(b) – Purpose Limitation

6.16 In order to comply with this principle the Council will:

- Clearly identify our purpose or purposes for processing the data
- Document those purposes in our Data Protection Register.
- Include details of our purposes in our privacy information to individuals.
- Regularly review our processing and, where necessary, update our documentation and our privacy information to individuals.
- If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we will check that this is compatible with our original purpose or get specific consent for the new purpose.

6.17 Article 5(1)(c) – Data Minimisation

6.18 In order to comply with this principle the Council will:

- Only collect personal data we actually need to the extent that is necessary to perform our functions and deliver our services.
- Collect sufficient personal data to properly fulfil those purposes.
- Periodically review the data we hold and delete anything we don't need.

6.19 Article 5 (1)(d) – Accuracy

6.20 In order to comply with this principle the Council will:

- Ensure as far as is practicable the accuracy of any personal data we create.
- Have appropriate processes in place to check the accuracy of the data we collect.
- Have appropriate processes in place to identify when we need to keep the data updated to properly fulfil our purpose.
- Ensure as far as is practicable the data is kept up to date (where required).
- Share personal data, 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.
- If personal data is found to be inaccurate, this will be remedied as soon as possible.
- If we need to keep a record of a mistake, we clearly identify it as a mistake.
- Our records will clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.
- Comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.
- As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.

6.21 Article 5 (1)(e) – Storage Limitation (Retention)

6.22 In order to comply with this principle the Council will:

- Not retain personal data for longer than is necessary it relation to the purpose for which it is processed.
- Have a Retention & Disposal policy/schedule that sets standard retention periods for records and data.
- Apply the Council's Retention & Disposal policy/schedule.
- Dispose of records that contain personal or confidential data in a secure way i.e. shredding, confidential waste and secure electronic deletion.

6.23 Article 5(1((f) – Integrity & Confidentiality (Security)

6.24 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 personal data is not transferred outside the UK without appropriate 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.

6.25 Article 5(2) – Accountability

Records of processing activity

6.26 The GDPR contains explicit provisions regarding the need for organisations to document their processing activities. Organisations must maintain records on several things such as processing purposes, data sharing and retention. Organisations may be required to make the records available to the ICO on request.

6.27 In order to discharge this key responsibility, the Council has in place a Data Protection Register (DPR). The DPR documents the following for each processing activity:

- purpose for processing
- legal basis for processing and supporting legislation
- categories of personal data processed
- categories of data subjects to which the data relates
- who the data is shared with (both internal and external partners)
- retention requirements
- information required for privacy notices
- records of consent
- controller-processor arrangements
- the location of personal data

6.28 Each register entry is subjected to regular review.

6.29 Privacy by Design / Data Protection Impact Assessments (DPIA)

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

- Undertake a DPIA for processing that is likely to result in a high risk to individuals.

- Adopt the ICO's screening checklist to determine when a DPIA is required.

- Develop a policy and procedure that documents the DPIA process.

6.31 Breaches of personal data

6.32 The GDPR requires 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.

6.33 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.

6.34 To comply with this requirement the Council has robust breach detection, reporting and investigation procedures in place that aims to ensure:

- Personal data breaches and information security incidents and events are detected, reported, categorised and monitored consistently.
- Breaches/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 of personal data are reported to the Information Commissioner within the required timeframe.
- Data subjects are notified if a breach of their personal data is likely to result in 'high risk'.
- Lessons learnt are communicated and actions to help prevent future incidents are agreed and monitored.

6.35 Data Protection Complaints

6.36 The Council is committed to dealing effectively with any complaints or concerns individuals may have about the way in which the Council processes their personal data.

6.37 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.

6.38 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, Rhondda Fach Leisure Centre, Tylorstown, CF43 3HR
e-mail: information.management@rctcbc.gov.uk

6.39 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
ico.org.uk
Telephone: 03031231113 or 01625545745

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

7.0 INFORMATION RIGHTS

7.1 The GDPR provides the following rights to individuals in relation to their personal data.

i. Right to access
This allows the individual to access and receive a copy of their personal data and other supplementary information.

ii. Right to correct incorrect information (rectification)
This allows the individual to ask the Council to have inaccurate personal data rectified or completed if inaccurate. This right is linked closely to the principle of accuracy (Article (5)(1)(d)).

iii. Right to erasure
This allows the individual to ask the Council to have their personal data 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 processing
This gives the individual the right to ask the Council to block or stop using their personal data if its continued use causes 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 data in a readable format so that it can be provided to another organisation or service provider. The right to portability applies in certain (limited) circumstances.

vi. Right to object
This right allows the individual to object to the Council processing their personal data where the processing is for direct marketing purposes.

Individuals can also object if the processing is for:

- a task carried out in the public interest;
- the exercise of official authority vested in you; or
- your legitimate interests (or those of a third party).

In these circumstances the right to object is not absolute.

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.

7.2 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 information rights requests.

8. ROLES AND RESPONSIBILITIES

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

8.2 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 Director of Finance & Digital Services is the Council's designated Senior Information Risk Owner (SIRO).

The SIRO is a key role within the Council that 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 Data Protection & Improvement Officer is the designated DPO for the Council. The DPO provides interpretation, advice and support on complex data protection and information governance 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 Service Director ICT & Digital. However, arrangements are in place whereby the DPO also has a direct reporting line to the SIRO in order to ensure organisational independence and objectivity.

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 (as reflected in the ICT & Digital Service Delivery Plan), monitors progress against the plan and provides assurance that information risk is being properly assessed, controlled and mitigated.

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:

- Data & Improvement Officer
- Deputy Data Protection Officer
- Senior Compliance Officer
- Compliance Officer

v. Head of Service (Information Asset Owners)

The role of the Information Asst Owner (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 data 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 principles of the GDPR.

vi. Employees (Information Users)

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

Individual Responsibilities:

- All employees must comply with this Policy. Failure to comply may result in disciplinary action which could lead to dismissal.
- Undertake relevant data protection training provided by the Council to support compliance with this policy.
- 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.

Appendix I

DEFINITIONS

GDPR	UK General Data Protection Regulation
DPA	Data Protection Act 2018
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: • race or ethnic origin, • political opinions, • religious or philosophical beliefs, • trade union membership • genetic data, • biometric data for the purpose of uniquely identifying a natural person, • data concerning health • data concerning a natural person's sex life or sexual orientation
Criminal Convictions	Whilst not classified as special category data by the GDPR, the processing of personal data relating to criminal convictions and offences carries specific instructions under Article 10 of the GDPR and also Schedule 1 of the DPA.
Data Subject	A Data Subject is a living individual to whom the personal data relates. Within the Council this could be a citizen, service user, customer 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 joint is used where two or more persons / organisations act together to decide the purpose and manner of any data processing

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.
Information Commissioner / Information Commissioner's Office (ICO)	The Crown appointed person (and department) responsible for the implementation and the policing of GDPR, DPA 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.

Appendix II

Document Control

Policy	ICT
Title	Data Protection Policy
Author	Data Protection & Improvement Officer
Owner	Service Director ICT & Digital
Initial Policy Launch Date	30.03.2018 (approved by Cabinet 22.03.2018)
Review date	This policy will be reviewed every two years of following any significant change in legislation (whichever is sooner).

Document Approvals

This document requires the following approvals:

1. Cabinet (initial policy and significant changes)
2. Information Management Board (revisions)

Version Control

Version No	Date Approved	Valid From Date	Valid To Date	Changes Made
1.0	22.03.2018 (Cabinet)	30.03.2018	13.12.2018	Final Document
1.1	13.12.2018 (IM Board)	13.12.2018	12.12.2019	Updated to reflect Data Protection legislation changes post 25/05/2018.
1.2	30.07.2019	30.07.2019		Change of Office Address Note – links updated 02.09.2021
2.0	01.11.2021	01.11.2021	21.02.2023	Full review to reflect changes in UK data protection regulation as a result of Brexit. Job titles and roles updated. Order of policy updated. Approved by Service Director Digital & ICT
2.1	21.02.2023	21.02.2023	17.01.2024	Footer added - Welsh version availability
2.2	17.01.2024	17.01.2024		Reviewed. Link to complaints policy updated.