Cornwall Council Data Protection Policy (v9.0)			
Author	Corporate and Information Governance	**Reviewed Date**	November 2019

1. Purpose

The purpose of this policy is to ensure Council staff apply appropriate measures to comply with the General Data Protection Regulation (GDPR) and in particular, but not solely, the six principles summarised below. This will help the Council meet its statutory requirements and mitigate penalties imposed by GDPR and the Data Protection Act 2018 (DPA) enforced by the Information Commissioner's Office (ICO).

The Council also wishes to ensure that the information it holds is both accurate and appropriate in order to facilitate good decision making. Holding out of date data is a breach of the data protection principles and could result in the Council receiving a fine and can lead to the Council making inaccurate decisions.

Article 5(1) of the GDPR requires that personal information (data relating to a living individual) 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 ('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 ('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 ('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')."

In order to process personal information lawfully there must be a legal basis to process:

- The individual has given the Council their clear consent;
- It forms part of a contract or pre-contractual negotiations between the Council and the individual;
- It is necessary for the Council to comply with a legal obligation (other than one imposed by a contract with the individual)
    - The processing must have a basis in law, the law should specify the type of personal data, the data subjects concerned, and storage period;
- It is in the vital interest of the data subject - applies only if it is a life or death situation;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council;
    - the administration of justice,
    - the exercise of a function conferred on a person by an enactment or rule of law,
    - an activity that supports or promotes democratic engagement.

Article 5(2) adds that:
"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

There are separate restrictions on processing data outside the EEA.

2. Scope

"Processing" is defined as any operation or operations performed on personal data, such as collection, recording, structuring, storing, alteration, retrieval, disclosure, combination, restriction erasure or destruction.

"Personal data" is defined as any information held about a living, identifiable individual. Individual identification can be by information alone or in conjunction with other information.

"Special category data" requires additional protection and is defined in GDPR as data about:

- Health
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where processed to identify a person)
- Sex life or sexual orientation

The processing of criminal offence data also has additional legal safeguards under DPA. Criminal offence data includes information about criminal allegations, criminal offences, criminal proceedings and criminal convictions.

This policy applies to personal, special category and criminal offences data held by the Council as defined in the GDPR and DPA 2018. Anyone who processes personal, special categories of personal information or criminal offences data for the Council must adhere to this policy.

Contractors who process personal, special category and criminal offences data on behalf of the Council must either adopt this policy or prove that they have equivalent policies in place.

3. Policy

3.1 Anyone who processes personal, special category or criminal offences data for, or on behalf of Cornwall Council will adhere to this policy and comply with GDPR and the Data Protection Act.

3.2 The Council has an appointed Data Protection Officer:
Data Protection Officer,
4N,
New County Hall,
Treyew Road,
Truro,
TR1 3AY
Tel: 01872 326424
Email: dpo@cornwall.gov.uk

3.3 Training:

3.3.1 All staff with a network account must complete the mandatory Information Governance e-learning package on an annual basis.

3.3.2 Non-networked staff must complete the paper based IG mandatory training on an annual basis.

3.3.3 Information Asset Owners must complete the Information Asset Owner training available to book through ERP.

3.3.4 The Senior Information Risk Owner (SIRO) and Caldicott Guardian must undertake annual training relevant for their role.

3.4 Breach reporting

All staff must immediately report any breaches of the Data Protection Act using the Council's Information Security Incident Reporting Procedure

3.5 Data subjects' rights

All staff must ensure that the Rights of access, rectification and erasure procedure (RARE) is followed for any requests for access, restriction or erasure of personal data.

3.6 Information Classification

All staff must ensure that personal data, special category and criminal offences data is labelled in line with Information Classification Policy

3.7 Business and Privacy Impact Assessments

All staff responsible for setting up or commissioning new services or procuring new systems must ensure that a Business and Privacy Impact Assessment (BPIA) is completed.

3.8 Contracts

Staff involved in procuring goods or services on behalf of the Council must ensure that a contract is in place where processing of personal data is carried out by third parties, either as a commissioned service, whether Cornwall Council is a data controller or joint data controller. The contract must include the approved Information Governance contract clauses.

If data is to be shared or made available to third parties where no contract exists (such as volunteers) a non-disclosure agreement (NDA) should be signed imposing obligations to refrain from disclosing information, taking measures to protect the confidentiality of information and/or using information only for a specified purpose or purposes.

3.9 Privacy notices and consent

All staff must be ensure that a privacy notice is made available at the point of collecting personal and special category data. If consent is being relied upon to process the data, mechanisms must be in place to enable consent to be withdrawn.

3.10 Sharing of personal data

All staff must ensure that there is a legal basis to share information prior to sharing the personal information with other services or partner organisations. The legal basis to share is likely to be linked to the legal basis for processing the information.

If consent is relied upon to process the data then consent to share the data must be requested and recorded, this must be made clear in the privacy notice and enable people to opt in to data sharing by listing all organisations the data will be shared with.

Any data sharing under statute must have a clear basis which is set out in legislation that covers either the United Kingdom or England. Both GDPR and the DPA18 allow data to be shared if this is allowed by law and the exact information sharing gateway from the legislation must be quoted in the information sharing agreement.

Information Asset Owners must ensure that an Information Sharing Agreement is in place to govern how information will be shared.

3.11 Information Asset Register

Every data set holding personal data must be assigned an Information Asset Owner and be included on the Information Asset Register (IAR).

The Information Asset Owner must:

- Ensure a BPIA is completed for every information asset;
- Ensure every information asset is included on the IAR;
- Complete a data flow map for each data set;
- Review the IAR entry and data flow map when processing changes and at least annually;
- Ensure data quality standards are in place and monitor adherence.

3.12 International transfers

If you are considering transferring data outside of the EEA you must contact the Corporate and Information Governance Team who will consider the following:

- Can the aims be achieved without sending the personal data? Consider anonymising the data;
- Is the receiving country covered by an "adequacy decision"?
- If data will be sent the U.S. the company must be covered by the Privacy Shield and the certification must cover the type of data planned to be transferred.
- If there is no adequacy decision "appropriate safeguards" (listed below) must be in place:
    - a legal instrument between two public authorities or bodies provided that the legal instrument provides 'appropriate safeguards' for the rights of the individuals whose personal data is being transferred and it is legally binding and enforceable;
    - binding corporate rules (BCRs);
    - standard contractual clauses' (sometimes as 'model clauses') which contain contractual obligations on the data exporter and the data importer, and rights for the individuals whose personal data is transferred.

4. Enforcement

4.1 The Data Protection Officer is the designated Council owner of the Data Protection Policy and is responsible for the maintenance and review of the Data Protection Policy, Standards, Guidelines and Procedures.

4.2 The Corporate and Information Governance Team in the Assurance Service, Customer and Support Services Directorate are responsible for overseeing day to day issues relating to data protection; developing and maintaining corporate data protection procedures, guidance and training.

4.3 The Customer and Information Governance Board reports on the status of compliance with Data Protection legislation to CDT.

4.4 The Council's Senior Information Risk Owner (SIRO) is responsible for managing corporate information risks, including maintaining and reviewing an information risk register.

4.5 The Council's Caldicott Guardian is responsible for protecting the confidentiality of service user personal information to ensure that standards are met when handling personal and sensitive personal information in health and social care.

4.6 The Employee Code of Conduct forms part of everyone's Contract of Employment and includes a commitment to protecting personal, special category and criminal offences data. Staff must only access personal, special category and criminal offences data that they are entitled to view as part of their role. Breaches of the GDPR or the Act could be regarded as gross misconduct and may result in disciplinary action up to and including dismissal. Staff may be personally liable for prosecution if they deliberately breach data protection legislation.

4.7 The Data Protection Officer will:

- Inform and advise the Council of its obligations and adherence to GDPR and DPA;
- Monitor compliance with GDPR and DPA, indicators to monitor the performance on compliance are:
    - The number of requests for Rights of Access, Rectification and Erasure and any failures on the part of the Council and/or its contractors to comply with these rights;
    - Statistics regarding information security incidents reported to the Senior Information Risk Owner, Directorate Leadership Teams and the Council Directors' Team.
- Assign responsibilities, raise awareness, staff training and related audits;
- Provide advice on Business and Privacy Impact Assessments;
- Liaise with the ICO
- Consider the risk associated with data processing operations.

Potential risks will be regularly monitored and evaluated to ensure this policy is kept up to date.

5. Exceptions

There are no exceptions to this policy.

6. Review

This policy will be reviewed annually or when legislation changes by the Data Protection Officer and passed to CIGB for approval.

7. Revision History

V0.1 (31.10.19) Draft for approval by CIGB

V9.0 (27.11.19) Approved by CIGB

8. Additional guidance

Cornwall Council Data Protection Policy (v9.0)			
Author	Corporate and Information Governance	**Reviewed Date**	November 2019

Information governance policies, procedures, guidance and references to training can be found on the Council's intranet if you search for Information Governance.