South Hams District Council

&

West Devon Borough Council

Data Protection Policy (2018)

Data Protection Policy (2018)

1. What is Data Protection?

The General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018 (DPA) apply to personal information that is held by the Council about living, identifiable individuals of any age. Examples of personal information includes an individual's contact information, details of the service we provide to the individual, recordings or photographs.

This personal information may be automatically processed, such as on a computer, smartphone, recording device or CCTV system, or in manual paper records, for example, hand-written meeting notes application forms, or printouts of what is held on computer.

Personal information includes information that has been 'pseudonymised' (a term used introduced by the GDPR where personal information has been removed from data); for example, information which has been given a reference number or code so that an individual cannot be identified, and the identifiable information is kept separately.

This Policy and associated Codes of Practice and Procedures are designed to promote and maintain compliance with the GDPR and the DPA. These two pieces of legislation work together in tandem; for example, the principles and requirements for handling personal information are set out in the GDPR, and exemptions, enforcement and penalties are set out in the DPA. The DPA also includes our obligations for processing personal information for law enforcement purposes.

2. When do the Data Protection rules apply?

The Data Protection rules apply to personal information about living, identifiable individuals who can be identified, directly or indirectly **wherever** that personal information is held, such as:

- Computer systems
- Audio recordings (such as telephone) or video recordings (such as CCTV)
- Mobile or smart phones
- Tablets or any device that can operate automatically in response to a set of instructions (such as a computer program). It does not matter whether the device is privately owned or owned by the Council. If the information held on it is used for Council purposes, then the Data Protection rules apply.
- Paper files that are structured (for example, alphabetically or in date order) and information can be easily accessed by looking up the name/address/postcode or other information about an individual.

- Paper records that are intended to be filed or transferred to computer, such as application forms.
- Unstructured paper records (for example, handwritten notes and jottings of a meeting that are not neatly filed away or indexed, nor transferred to computer).
- Expressions of opinion and intentions (for example, views expressed about someone in an email message).

Ultimately, if the Council obtains, holds or does something with personal information the Data Protection rules apply.

The Data Protection rules **do not apply** to:

- De-personalised, anonymised or statistical information where individuals cannot be identified;
- Businesses or organisations (unless it relates to a sole trader or partner in a business partnership)
- People who are deceased, although the DPA applies to those who remain. For example, there is a duty of confidentiality to those who may be named on the deceased's records.

3. The Data Protection Principles

These are legally enforceable principles and requirements which are the foundation of good information management and help us to respect the rights of individuals.

The **GDPR Principles** require that personal information must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the information is processed ('storage limitation').
- 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').
- Accountability: the controller (the Council) is responsible for, and must demonstrate compliance with the Principles.

- Individuals' rights and access to personal information must be upheld, including the right to:

    - be informed about what we do with his/her information
    - rectification
    - erasure / right to be forgotten
    - restriction of processing
    - data portability (i.e. the right to be provided with personal information in a structured, commonly used machine-readable format)
    - make an objection
    - Not to be subject to a decision based on automated individual decision-making and profiling

- Only transferring personal data to countries, territories or international organisations outside the European Union if there are adequate protections in place or safeguards.

4. How do the Regulations and Data Protection Act affect me?

The GDPR and DPA rules apply to anyone in the Council who has access to, uses or passes on personal information in his/her day-to-day work.

Breaches of the Principles may result in the Council facing substantial monetary penalties, being publicly named-and-shamed, and would result in the loss of trust from the people we provide services to.

For employees, it is a criminal offence to:

- Obtain, procure, handle, disclose or retain personal information without the Council's authorisation or consent

- Sell (or offer to sell) personal information that has been unlawfully obtained, which includes advertising it for sale.
- Re-identify personal information that has been de-identified.
- Alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the requestor is entitled to receive.
- Force someone to make a subject access request to see information about their convictions, cautions, health records or Disclosure Barring Service information, as a method of vetting them.

5. What is the Council's Data Protection Policy?

The Council's aims are to make every effort to ensure:

- Compliance with the GDPR and DPA is maintained

- Personal information is well-managed, held securely and that the rights of individuals are respected.

- Data protection is integrated into the Council's working practices and information systems from the moment information is collected through to its destruction.

- Compliance with the accountability principle, being responsible for and able to demonstrate compliance with the other principles and requirements, such as:
    - Implementing appropriate technical and organisational measures such as internal data protection policies, procedures and codes of practice, staff reporting, provision of staff training, internal audits of processing activities, and reviews of internal Human Resources policies.
    - Maintaining documentation of our processing activities.
    - Appointing a Data Protection Officer.
    - Implementing measures that include:
        - Data minimisation
        - Pseudonymisation
        - Transparency
        - Allowing individuals to monitor processing
        - Creating and improving security features on an ongoing basis.
    - Conducting Data Protection Impact Assessments where appropriate.

This Policy is supported by the Senior Leadership Team (SLT) and commits the Council to providing the necessary resources to ensure that this Policy's aims can be achieved.

Procedures that describe the arrangements and processes for the implementation of this policy will be available on the Council's intranet.

6. Who is Responsible for Data Protection?

Data Protection Officer

The Council has appointed a Data Protection Officer (the DPO), Darren Arulvasagam.

The DPO reports to the Audit Committee (who will make any necessary recommendations to the Council) and is responsible for:

- Ensuring the objectives of the Data Protection Act 2018 and related legislation are achieved and assisting the Council with its compliance and maintaining standards of good practice.

- Ensure the objectives of the Information Governance Group are achieved, managing it and reporting progress to SLT.

- Providing advice to the Council for the resolution of queries and maintaining the accuracy of the Council's internal **Record of Processing Activities** and keeping it up to date.

- Managing data protection procedures, policies, codes of practice and revised documentation.

- Arranging training opportunities for employees and elected Members.

- Constructing and reviewing compliance monitoring programmes; ensuring their completion and reporting findings

Information Governance Group
To ensure that the Council complies with all relevant legislation and best practice in relation to:

- Data Protection
- Freedom of Information
- Environmental Information
- Records Management / Document Retention
- Data Security

The Information Governance Group will meet regularly to maintain an overview, consider issues, monitor compliance and arrange for necessary action to be taken.

The Information Governance Group will:

- Ensure consistency and compliance with legislation and best practice
- Ensure that the Council develops and maintains corporate policy, procedures, and codes of practice
- Develop guidance for staff and Members
- Commission training for all Officers and Members
- Obtain specialist help when required
- Monitor and review performance to ensure compliance and improvement
- Devise a work plan

Managers and Service Area Leads
Have overall responsibility for ensuring that personal information held within their service area is managed in a way which meets the aims of the Council's Data Protection Policy.

They should ensure that all staff responsible for managing personal information are appropriately trained or experienced and understand the need for Data Protection.

All Staff
All staff who create, receive and use personal information have responsibilities under this Policy, Council Codes of Practice and to comply with the requirements of the GDPR and DPA.

It is the responsibility of managers to ensure that anyone who is sub-contracted or employed on a temporary or voluntary basis is made aware of this Policy, Codes of Practice and any relevant supporting procedures that are available.

Where personal data is disclosed to our service providers or anyone else acting on our behalf, they will ensure that there is a written contract in place that includes the requirement for them to comply with the GDPR and DPA (in particular the Security Principle).

7. What happens if I contravene this policy?
Disciplinary action, including dismissal, may be taken against any member of staff who contravenes this Data Protection Policy and supporting Codes of Practice and Procedures.

On discovering that this Policy is not being complied with, or if an intentional breach of the Data Protection Principles, Undertaking, or criminal offence has taken place under the GDPR and DPA, the Data Protection Officer shall have full authority to take such immediate steps as considered necessary.

8. Is this policy linked to any other policies and procedures?
This policy is linked to the following policies and information which are available on the Council's website:

- ICT Policy
- Freedom of Information Policy
- Regulation of Investigatory Powers Act Policy
- Records Management Policy
- Complaints Policy

Is there any guidance to help?
You can find further help by:

- Looking at the various Codes of Practice on different aspects of Data Protection which are available on the Council's website

- Look at the guidance on the Information Commissioner's website

- Ask for further guidance from the Information Governance Group

- Contacting the Data Protection Officer via email to data.protection@swdevon.gov.uk

9. Will this policy be monitored or reviewed?

Compliance with the Data Protection Policy will be monitored by the DPO and Information Governance Group and reviewed every three years or earlier if required.

This Data Protection Policy has been authorised by the Data Protection Officer and approved by Members on ***tbc*** date 2018

Signed …….. Date …….

Data Protection Officer