Swindon Borough Council GDPR Data Protection Policy

1. Introduction

Swindon Borough Council supports the objectives of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) and seeks to ensure compliance with this data protection legislation.

The processing of data by the Council is essential to services and functions and will often involve the use of personal and/or 'special category' personal data. Compliance with the data protection legislation will ensure that such processing is carried out fairly and lawfully.

The GDPR and the Human Rights Act (1998) (HRA) Article 8, make it clear that the processing of personal data must respect the rights and freedoms of the data subject (individual), but at the same time be adequate enough for the councils to function effectively.

This policy should not be read in isolation and regard should be given to all other Council policies.

2. Purpose

The purpose of this policy is to ensure that the provisions of the GDPR and DPA are adhered to whilst protecting the rights and privacy of living individuals; ensuring their personal data is not processed without their knowledge.

In particular this policy will:

- Assist the Council to comply with all requirements of the GDPR and DPA.
- Ensure that personal data is readily available on request and that requests from data subjects are dealt with in a timely manner.
- Ensure adequate consideration is given to whether or not personal information should be disclosed.
- Ensure increased awareness of data subjects to the amount of personal data processed and stored by the council about them and advise them of their rights under the data protection legislation.

The Council will endeavour to promote greater openness, provide increased transparency of data processing and build public trust and confidence in the way that it manages information about customers, service users and data subjects.

3. Aims

This policy sets out the Council's commitment to upholding the data protection principles set out in the GDPR and managing information held fairly and lawfully. It seeks to strike an appropriate balance between the Council's need to make use of personal information in order to manage services efficiently and effectively and respect for the privacy of individuals.

To assist staff to meet their statutory obligations under the GDPR and DPA and provide a guide to the public on the Council's obligations with regard to the processing of their personal data.

4. Council data protection requirements

This policy applies to the acquisition and processing of all personal data within the Council and sets out how the Council will ensure that individual rights and freedoms are protected.

The Council will comply with Article 8 of the HRA in respect of the processing of personal data.

The Council, as the Data Controller, will make individuals aware of the purpose(s) it is processing their personal data for and will always seek consent where appropriate.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

The Council will provide general information to the public about their statutory rights under the GDPR and DPA on our website.

The Council will hold the minimum amount of personal data necessary to carry out its functions, and every effort will always be made to ensure the accuracy and relevance of data processed.

The Council will keep its electronic and manual records and all personal data in accordance with the six principles of the GDPR and in line with the Council's Retention and Disposal Policy.

Periodically, a Privacy Impact and Risk assessment (PIA) will be undertaken for all data processing, and always when new processing of personal data is being planned. If inadequate controls are identified, then technical and organisational security measures will be put in place, appropriate to the level of risk(s) identified.

Personal data will only be used for the direct promotion or marketing of goods or services with the explicit consent of an individual.

Data sharing, disclosing and matching with external agencies will only be carried out under a written contract or agreement setting out the scope and limits of the data processing.

Elected Members and staff will be trained to an appropriate level in the use and supervision of personal data.

Any breaches of this policy may be subject to action under the Council's disciplinary procedures.

The Council will abide by the six data protection principles as detailed below:

Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
2. 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, in accordance with GDPR Article 89(1) not be considered incompatible with the initial purposes ('purposed limitation')
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
4. 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')
5. 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 in

accordance with GDPR Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

6. 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. Roles and responsibilities

The Council's Corporate Management Team (Information Governance Board) is responsible for approving this policy for managing compliance with the GDPR and DPA.

Overall responsibility for the GDPR and DPA will rest with the Chief Executive, in consultation with the Data Protection Officer (Information Governance Manager) and Senior Information Risk Owner.

The Council's Data Protection Officer (Information Governance Manager) is responsible for the provision of advice, guidance and training regarding data protection legislation and will be responsible for keeping this document up to date.

All employees, in consultation with the Information Governance Team, will be responsible for ensuring that Subject Access Requests are dealt with in accordance with this policy and that personal data is processed appropriately. This includes ensuring that personal data supplied to the Council is accurate, up-to-date and held appropriately securely.

Heads of Service and Information Asset Owners will be responsible for ensuring operational compliance with this policy within their own service areas and for becoming involved in consultations with the Information Governance Manager when applicable.

Internal Audit will undertake reviews to assess the procedures and policies in place that relate to data protection.

6. Information requests

Requests from data subjects for copies of personal data the Council holds about them (Subject Access Requests) can be made in writing or verbally. This includes requests transmitted by electronic means, providing they are received in a legible form and are capable of being used for subsequent reference.

If a person is unable to articulate their request in writing, we will provide advice to assist them in formulating their request.

If the information sought is not described in a way that would enable the Council to identify and locate the requested material, or the request is ambiguous, the Council will always seek additional clarification.

The Council will not provide assistance to any applicant who is not the data subject, unless it is confirmed that the explicit consent of the data subject has been obtained for the third party to act on their behalf and to request the data subject's personal data.

7. Prompt replies to requests

The Council is committed to dealing with requests for personal data promptly and unless otherwise arranged, no later than the statutory guideline of one calendar month. If the Council considers the

request to be complex, it may extend the time for providing the information by up to two additional calendar months.

In such an instance, the Council will notify the applicant in writing that the request requires further time and will provide an estimate of a 'reasonable time' by which they might expect a response to be made.

These estimates shall be realistic and reasonable taking into account the circumstances of each particular case.

8. Data subject rights

Subject to some exceptions, individuals will have the rights below.

- Right to request a copy of any information we hold
- Right to rectification (if inaccurate data is held)
- Right to erasure ('right to be forgotten') in certain circumstances
- Right to restriction of processing in certain circumstances
- Right to data portability (personal data transferred from one data controller to another)
- Right to object (to profiling, direct marketing, automated decision-making)

9. Exempting information from non-disclosure

The GDPR is designed to prevent access by third parties to a data subject's personal data. However, under the DPA there are circumstances which allow disclosure of a data subject's personal data to a third party, or for it to be used in a situation that would normally be considered to breach the GDPR.

Exemptions from the non-disclosure of personal data are given below. This list is not exhaustive.

Crime and taxation: general

- the prevention and detection of crime
- the apprehension or prosecution of offenders, or
- the assessment or collection of any tax or duty or of any imposition of a similar nature

Crime and taxation: risk assessment systems

- Immigration
- Information required to be disclosed by law etc. or in connection with legal proceedings

The Council will only use these exemptions where it is in the public interest to do so, i.e. prevention of crime, or where the functioning of the Council requires the processing of personal information to be exempt so that it can provide statutory services to members of the public.

10. Refusal of subject access requests

The Council will not supply information to a data subject if:

- We are not satisfied with the identity of the data subject
- Compliance with the request will inadvertently disclose personal information relating to another individual without their consent
- The applicant has recently requested the same or similar information

- The Council considers that a valid reason, which is both robust and legally defendable, exists for refusing the disclosure of information to either the data subject or a third party, the information should be withheld.
    - When such information is withheld, a full explanation of the reasoning behind the refusal must be provided to the applicant. This explanation must also include full details of how the applicant can complain about the Council's decision.

All requests for personal data made by data subjects will be dealt with under Chapter 3 - Rights of the Data Subject section of the GDPR, not the Freedom of Information Act 2000.

11. Appeals and complaints

Where an applicant is dissatisfied with the level of service they have received, they are entitled to complain about the actions of the council through the internal appeals procedure.

All complaints should be sent to:

Data Protection Officer

Swindon Borough Council

Euclid Street

Swindon

SN1 2JH

Alternatively, by email to::DataProtection@swindon.gov.uk

The applicant will receive a response to their correspondence within twenty working days. If the applicant remains dissatisfied with the Council's reply, they have the option of taking their complaint to the Information Commissioner (at the address below) who will independently adjudicate each case and make a final decision.

Information Commissioner's Office

Wycliffe House,

Water Lane

Wilmslow

Cheshire

SK9 5AF

Alternatively, by email to: casework@ico.org.uk or by phoning: 01625 545700

Appendix 1

Interpretation of Terms

1. ‘Personal data’ means any information relating to an identified or identifiable living individual (‘data subject’)

2. ‘Identifiable living individual’ means a living individual who can identified, directly or indirectly, in particular by reference to:
   - an identifier such as a name, an identification number, location data or an online identifier, or
   - b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

3. ‘Special category (sensitive) personal data’ means:
   - Racial or ethnic origin
   - Political opinions
   - Religious/philosophical beliefs
   - Trade union
   - Processing of biometric/genetic data to identify someone
   - Health
   - Sex life or sexual orientation

4. ‘Processing’, in relation to personal data, means an operation or set of operations which is performed on personal data or on sets of personal data, such as:
   - collection, recording, organisation, structuring, storage
   - adaptation or alteration
   - retrieval, consultation, use
   - disclosure by transmission, dissemination or otherwise making available
   - alignment or combination, or
   - restriction, erasure or destruction.

5. ‘Data subject’ means the identified or identifiable living individual to whom personal data relates.

6. ‘Controller’ means 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.

7. ‘Processor’ means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

8. ‘Filing system’ means any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.

9. ‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear

affirmative action, signifies agreement to the processing of personal data relating to him or her.