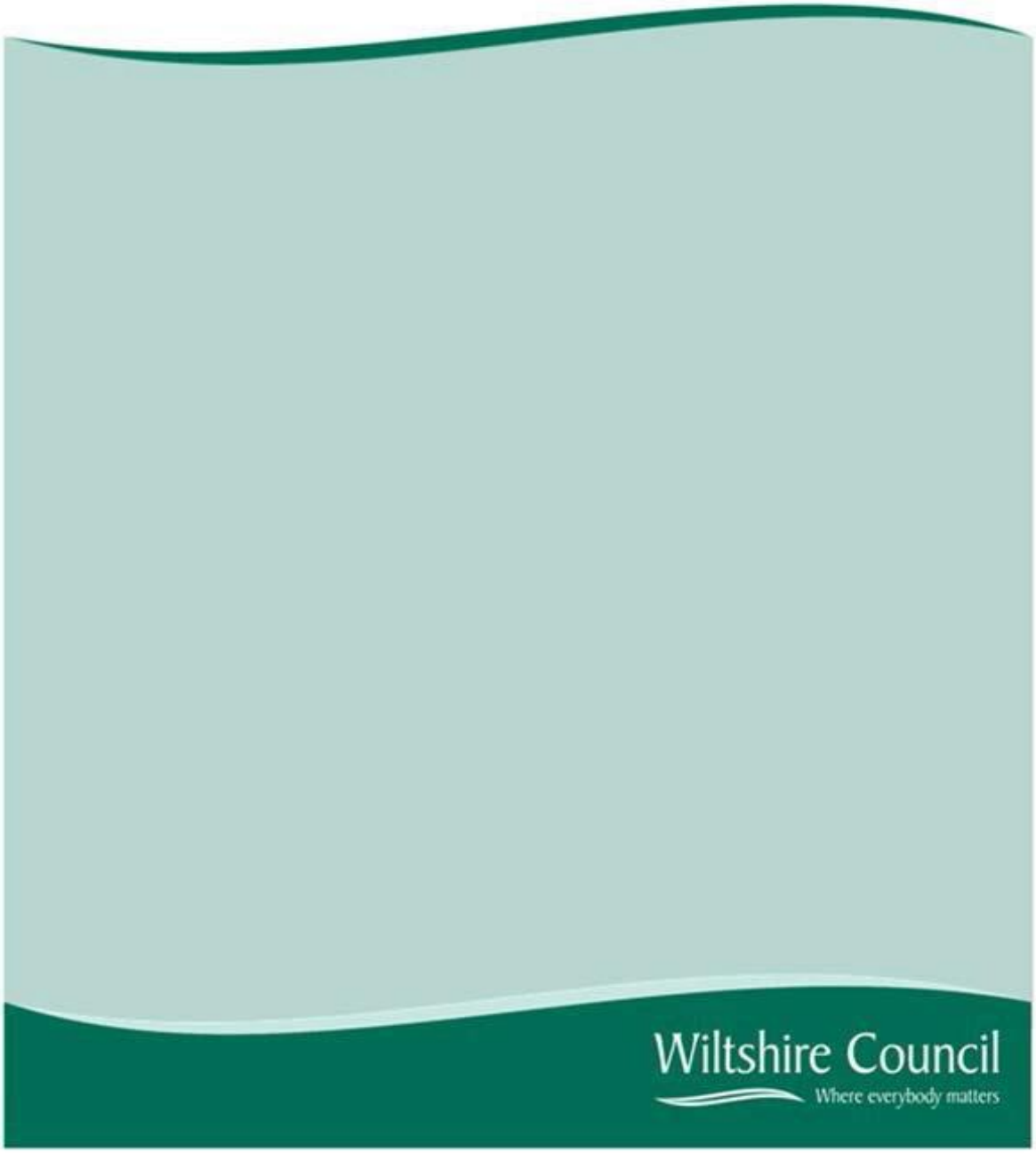
Data Protection & Subject Access Policy



Document Control

Reference Number	**Version** 3	**Status** Published	**Sponsor(s)/Author(s)** Andrew Holyoake Data Protection Lead
Amendments			
Document objectives: To ensure compliance with statutory requirements in relation to the processing of personal information across the Council. To provide guidance on data subjects' right to access their own information.			
Intended Recipients: Wiltshire Council Officers, temporary staff, Volunteers, Elected Members, and members of the public.			
Group/Persons Consulted: None			
Monitoring Arrangements and Indicators None			
Training/Resource Implications:			

Ratifying Body and Date Ratified	Information Governance Board
Date of Issue	V3.0 June 2018 April 2018
Review Date	March 2019
Contact for Review	Information Governance
SIRO signature	

Policy on a page

- This policy provides the Council's standards to be maintained to comply with the UK Data Protection Act 2018 (DPA) and EU General Data Protection Regulation 2016 (GDPR), and signposts to further guidance.
- This document will be distributed to: All Elected Members, Council Staff, 3rd Party Contractors, Secondees and Volunteers.

Key Messages

- Wiltshire Council (WC) is defined as a data controller and as such all Council Members, Officers, Contractors and Volunteers have a responsibility for data protection.
- You must read, understand and comply with the Information Governance Corporate Policy Framework and guidance to be found on the intranet.
- Data protection applies to all the personal and "sensitive" special category data held by, and on behalf of the Council. This information must be lawfully and fairly processed and where required explicit consent must be obtained and recorded.
- You must only access personal data, client records, files and folders which you "need to know" in order to do your job. Unauthorised access is a criminal offence.
- Safeguarding of people, at immediate risk of harm, over-rides data protection concerns.
- All members of the public and employees, as data subjects, have statutory rights including the right to know what information we hold and to obtain a copy of that information.
- You must complete annual Information Governance refresher training and sign up to the Confidentiality Agreement that is contained within it.
- You must report any suspected data breach of personal data to your line manager immediately, and in any case within 24 hours of becoming aware of the breach.
- Make yourself aware of the additional statutory responsibilities on the Council, including the need for Privacy Notices, Data Processing Contracts, Records Management, Data Protection Impact Assessments, the Council Data Protection Officer, RIPA (Covert Surveillance), PCIDSS (Payment Card regulations) where appropriate to your role.

This "policy on a page" is a summary of the detailed policy document please ensure you read, understand and comply with the full policy

Associated Documentation

Policies - Wiltshire Council controlled documents

- Information Governance Policy
- Information Security Policy
- Password Policy
- Records Management Policy
- Acceptable use policy
- Breach Reporting procedure
- Subject Access Request Process
- Wiltshire Information Sharing Charter
- Information Sharing Policy

Legal framework

- EU General Data Protection Regulation 2016
- Data Protection Act 2018
- Human Rights Act 1998
- Criminal Justice and Immigration Act 2008

Contents

1 Policy Statement

1.1 Wiltshire Council will ensure every user is aware of, and understands, their responsibilities regarding the security of personal data held by, and on behalf of, the Council in respect of;

a) their responsibilities under data protection law for the protection of personal data

b) the benefits of appropriate data sharing

c) the necessity for good records management

d) the technical and administrative controls operating in the Council

e) other laws and statutory guidance around this subject

1.2 Wiltshire Council holds and processes information about its employees, clients, and other individuals for various purposes. To comply with the General Data Protection Regulation 2016 (the GDPR), information must be collected and used fairly, stored safely, securely disposed of, and not disclosed to any unauthorised person.

1.3 The GDPR and this policy apply to all personal information processed by the council. Non-compliance with this policy may result in disciplinary action.

1.4 Any work activity involving personal data now has the status of a regulated activity.

2 Scope

2.1 This policy is intended for all Councillors, Committees, Services, Partners, Employees of the Council, Contractual Third Parties and Agents of the Council who have access to information held or processed by Wiltshire Council.

2.2 This policy covers all personal information held by the Council however it is collected, recorded and used, whether digital, on paper or recorded on other media.

2.3 This policy covers records held and processed by the council. The council is responsible for its own records under the terms of the GDPR, and it has submitted a notification as a Data Controller to the Information Commissioner. Registration No. Z1668953

3 Summary of Aims

3.1 The lawful and correct treatment of personal information is vital to the successful operation of, and maintaining confidence within the council, and the individuals with whom it deals.

3.2 Therefore, the council will, through appropriate management, and strict application of criteria and controls:

a) Observe fully conditions regarding the fair collection and use of information;

b) Meet its legal obligations to specify the purposes for which information is used;

c) Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;

d) Ensure the quality of information used;

e) Apply strict checks to determine the length of time information is held;

f) Take appropriate technical and organisational security measures to safeguard personal information;

g) Ensure that personal information is not transferred abroad without suitable safeguards.

h) Ensure that the rights of people about whom information is held can be fully exercised under the GDPR. (These are set out in in Articles 13 to 22 of the General Data Protection Regulation 2016 and include:

i. The right to access your personal information, to request rectification or erasure of certain personal information and to object to processing in certain circumstances.

ii. The right to withdraw any consent you may have given to process your personal information.

iii. The right to complain to the Information Commissioner if you feel we are processing your personal information unlawfully.

iv. The right to restrict processing activity in certain circumstances.

v. The right to object to certain types of processing activity such as automated decision making and profiling.

4 Notification to the Information Commissioner

4.1 The council has an obligation as a Data Controller to notify the Information Commissioner of the purposes for which it processes personal data.

4.2 Notification monitoring within the council is carried out by the Data Protection Officer.

4.3 Individual data subjects can obtain full details of the council's data protection registration/notification with the Information Commissioner from the Information Governance Manager or from the Information Commissioner's website (ico.org.uk).

4.4 Wiltshire elected Councillors are required to register as data controllers for their individual constituency casework. This is a personal obligation.

5 Council staff with Data Protection responsibilities

5.1 All queries about this council policy should be directed to the Data Protection Officer.

5.2 Requests for a subject access request should be made to the Information Governance Team.

5.3 See also Section17 Right of Access to Personal Data for more details.

6 Data Protection Principles

6.1 The council, as a Data Controller, must comply with the six Data Protection Principles set out in the GDPR. In summary, these state that personal data shall be:

a) processed lawfully, fairly and in a transparent manner

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

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;

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').

6.2 The Council is responsible for, and must be able to demonstrate compliance with the above principles.

7 Processing

7.1 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as:

a) collection,

b) recording,

c) organisation,

d) structuring,

e) storage,

f) adaptation or alteration,

g) retrieval,

h) consultation,

i) use,

j) disclosure by transmission, dissemination or otherwise making available,

k) alignment or combination,

l) restriction,

m) erasure or destruction;

8 Privacy Notices and Data Subject Information notices

8.1 Any collection of personal data must satisfy the requirements of fairness and transparency set out in the first Principle.

8.2 This includes paper or electronic application forms, telephone calls, and surveys.

8.3 At the time of collection, the Council will provide data subjects with information to comply with Articles 13 & 14 of GDPR. This shall explain to the individual:

a) The identity of the Data Controller collecting the information – Wiltshire Council

b) Contact details for the Council and its Data Protection Officer dataprotection@wiltshire.gov.uk

c) The purpose for processing and the legal basis for doing so

d) Recipients or categories of recipients of their personal data

8.4 Wiltshire Council will ensure an appropriate Privacy Notice is included wherever personal data is collected.

8.5 Wiltshire Council publishes an overarching Privacy Notice is in a prominent position on the web sites it maintains. In addition, where services have different specific needs, further privacy notices which are service specific will be added where appropriate.

9 Responsibilities of Individual Data Users

9.1 All employees and Members of the council who record and/or process personal data in any form (called "Data Users" in this policy) must ensure that they comply with:

a) The requirements of the General Data Protection Regulation 2016 (including the Data Protection Principles);

b) The council's Data Protection Policy, including any procedures and guidelines which may be issued from time to time.

9.2 A breach of the General Data Protection Regulation 2016 and/or the council's Data Protection Policy may result in disciplinary action.

9.3 Consideration should be given towards contacting the Information Governance Team for data protection advice concerning the following:

a) When developing any new system for processing personal data - it may also be necessary to comply with the council's Information Asset Change Policy and Data Privacy Impact Assessment Policy;

b) When using an existing computer system to process personal data for a new purpose as it may be necessary to notify an amendment to an existing registration in the council's Information Asset Change Policy, and it will be necessary to document the new processing activity;

c) When creating a new manual filing system containing personal data;

d) When using an existing manual filing system containing personal data for a new purpose.

10 Contractors and Data Processors

10.1 Outside agents working with Wiltshire Council data will be required to ensure full data compliance in accordance with contractual arrangements. Wiltshire Council reserves the right to inspect contractors and data processors to satisfy these requirements.

11 Accuracy of Data

11.1 Staff that have responsibility for handling any client, staff or other individual's personal information must ensure that it is accurate and as up to date as possible.

11.2 All staff members are responsible for checking that any personal information they provide to the council in connection with their own employment is accurate and up to date e.g. change of address or name.

11.3 The council cannot be held responsible for issues arising from any errors in such employment data unless the member of staff has informed the council about any relevant changes of circumstance.

12 Special Category Data

12.1 The council will process "special category data" relating to staff, clients, contractors and other individuals. This category of personal data may include information which has incidentally come into the possession of the council.

12.2 The council may need to process information regarding criminal convictions or alleged offences in connection, for example, with any disciplinary proceedings or other legal enforcement obligations. Such processing will be in accordance with the provisions of the Data Protection Act 2018

12.3 In circumstances where sensitive personal data is to be held or processed, the council will seek the explicit consent of the individual in question unless another legal basis to process applies (such as to perform a legal duty regarding employees, to protect the data subject's or a third party's vital interests or if it is necessary for the purposes of the provision or management of health or social care services).

13 Data Protection Impact Assessments (DPIA)

13.1 The Council must carry out a DPIA in all decision-making processes and projects where personal and special category data is used. Guidance on DPIAs is available online.

14 Data Security and Disclosure

14.1 All staff within the council are responsible for ensuring that any personal data which they hold is kept securely, and that personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party. Every reasonable effort must be made to ensure that data is not disclosed accidentally.

14.2 Deliberate unauthorised disclosure is a disciplinary matter and may be considered gross misconduct. Such deliberate action also has the potential to be a criminal offence. If in any doubt, consult the Information Governance Manager, Data Protection Officer, or Human Resources. Personal data must be kept securely and examples of how this may be done will include:

14.3 Keeping the data in a locked filing cabinet, drawer or room; or if the data is computerised, ensuring that the data is password protected or kept on a secure network and only where necessary as a temporary measure on secure removable media.

14.4 Any other appropriate security measures which are detailed in the council's IG policy section of the internal web, such as clear desk policy, confidential waste disposal and guidance on secure transfer of personal information and meeting held in public places.

14.5 Information Sharing Agreements will be required to facilitate regular and routine sharing of personal information with external organisations and partner agencies. All other information sharing will need to be justified in accordance with data principles and documented in compliance with the Information Sharing policy.

15 Data Breaches & Security Incidents

15.1 If you are aware that you, or someone else, has disclosed personal or sensitive data, to someone who did not have permission or authority to receive that information, you must report it to your line manager or the IG Team immediately and **in any case within 24 hours of discovery**:

a) If any personal information has been sent to the wrong individual, in paper form, attempts must be made to recover the information, ideally in person.

b) If any personal information has been sent to the wrong individual, in electronic form, attempts must be made to ensure the recipient has deleted the information from their computer and email.

c) Your line manager must ensure a report is sent to to the IG team to ensure they have all the necessary information in case the breach needs to be notified to the Information Commissioner's Office (ICO) within 72 hours.

15.2 The mandatory process that governs how that data breach is dealt with is covered in detail in the Council's Data Incident Reporting Policy.

16 Consent

16.1 Only when no other lawful basis to process can be identified, will the council will seek consent from data subjects to process their personal information.

16.2 Care should be taken not to confuse consent to receive a service or package of services or benefits, with consent to process data. GDPR principles are only concerned with consent to process data.

16.3 Consent will not be regarded as valid unless it can be demonstrated to be fully informed, freely given, and an unambiguous positive indication that the data subject knows what they are consenting to and why.

16.4 Consent must be as easy to refuse or withdraw as it is to give. If consent to process is withdrawn, only once another legal basis has been established may processing restart or continue

17 Right of Access to Personal Data

17.1 All individuals have the right under the GDPR to access any personal data that is being held about them. They also have the right to request the correction of such data where they are inaccurate.

17.2 The council has a Subject Access Process for manging requests for information. An individual who wishes to exercise his/her right of subject access is required to request this information in writing to the council.

17.3 Subject Access requests shall only be responded to by trained staff under guidance from Information Governance personnel. Every effort shall be made to comply within the 30 calendar day statutory time limits.

17.4 Any inaccuracies in data which are highlighted as a result of disclosure in this way should be communicated immediately to the Information Governance Manager, or Senior Information Governance Lead who shall take appropriate steps to have the necessary amendments made by the relevant service.

18 Access to Third Party Personal Data by Elected Representatives

18.1 Currently, under the Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002, MPs and Members of Wiltshire Council can make a request for (sensitive) personal information about someone if they are acting in an official capacity on behalf of a constituent, and this personal information may be provided without the council receiving explicit consent from the data subject in question.

18.2 Any further onward disclosure of information supplied to a Councillor must be in compliance with data principles, and in particular must be fair, lawful and justified by reference to the first data principle. Responsibility for confirming that such processing activity is compliant lies with the relevant Councillor.

18.3 It is anticipated this Order will fall on 25th May 2018 but at the time of going to press no replacement is forthcoming. Any provision of special category data to an elected member or particularly an MP should therefore be referred to the Information Governance team who will engage with the member and service to facilitate an appropriate solution.

19 Complaints

19.1 Complaints resulting from disclosure of personal information must be referred to the Data Protection Officer or Information Governance Manager who will be responsible for investigating them and preparing an appropriate response.

20 CCTV

20.1 A number of CCTV cameras are present on the council sites, to assist with security for staff, other individuals and their property, and in accordance with the council's 'notification' to the Information Commissioner.

20.2 Disclosure of images from the CCTV system will be controlled and consistent with the purpose for which the system was established. For example, it will be appropriate to disclose images to law enforcement agencies if necessary to support a criminal investigation but it would not necessarily be considered appropriate to place images of identifiable individuals on the internet or disclose them to the media for entertainment purposes.

20.3 Images can be released to the media for identification purposes; however, this should not generally be done by anyone other than a law enforcement agency.

20.4 If you have any queries regarding the operation of or access to the CCTV system, please contact the council Security Manager.

20.5 If access is required in connection with ongoing disciplinary matters, permission should be sought from the Head of Human Resources or their nominated deputy.

21 Covert Surveillance – Regulation of Investigatory Powers Act (RIPA)

21.1 The Council does not in general operate under the remit of RIPA, however if you are doing any of the following please contact Information Governance for advice and guidance to ensure compliance with the law.

a) Use of private investigators

b) Use of cameras or sound recordings to monitor members of the public

c) Use of Facebook or other Social Media to trace or monitor members of the public

d) Use of Social media to screen or assess prospective or current employees

22 Travelling Abroad

22.1 If you intend to travel abroad for work or you are taking your Corporate laptop or mobile phone abroad you must contact the ICT helpdesk or Information Governance who will advise you. Different countries have a variety of controls and restrictions on travelling with encrypted devices.

23 24:- Email

23.1 It is permissible and appropriate for the council to keep records of internal communications, provided such retention complies with the Data Protection Principles.

23.2 All council staff should be aware that the GDPR subject access right, subject to certain exceptions, also applies to emails which contain personal data about individuals which are sent or received by council staff.

24 Disclosure outside of the United Kingdom (UK) or European Economic Area (EEA)

24.1 The council may, from time to time, need to transfer personal data to countries or territories outside of the European Economic Area (which is the EU member states plus the European Free Trade Association (EFTA) countries of Iceland, Liechtenstein and Norway) in accordance with purposes made known to individual data subjects.

24.2 However, such a transfer will only be lawful if it is to a destination which has been declared a safe and secure destination. This is called transfer of data on the basis of an adequacy decision. It is a presumption that any country implementing GDPR will have adequacy, and other countries may have adequacy decisions determined in their favour such as the USA.

24.3 If you are considering transferring data to another country, outside of the EEA please consult the Information Governance team first – before any such transfer.

24.4 If an individual wishes to raise an objection to disclosure, then written notice should be given to the council's Data Protection Officer.

24.5 Other personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the EEA to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects.

24.6 The European Commission has the power to determine whether a third country (i.e. not an EU member state or an EFTA country) ensures an adequate level of protection for personal data by reason of its domestic law or the international commitments it has entered into.

24.7 The Commission has so far recognised Switzerland, Canada, Argentina, Guernsey, Isle of Man, Jersey, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection.

25 Retention of Data

25.1 The council will hold different types of information for differing lengths of time, depending on legal and operational requirements, following which it will either be archived or destroyed.

25.2 This will be done in accordance with the retention periods detailed in the council's retention schedule which is compliant with the National Archives guidance, the Code of Practice for Management of Records, Section 46, Freedom of Information Act (2000) and the relevant legislation.

25.3 All data retention will comply with the 5th Principle of Article 5 of GDPR Retention schedules are published online.

26 Training

26.1 All staff will receive mandatory training on data security, data principles, and general compliance with the GDPR. This training will be repeated at regular intervals and tailored to meet different needs of the various council service areas.

27 Appendix EEA Countries

27.1 Article 44 of the General Data Protection Regulation 2016 prohibits the transfer of personal information to countries or territories that do not meet adequacy requirements. GDPR applies to members states of the European Economic Area (EEA).

27.2 Currently the EEA consists of the 27 European Union member states and 3 other states. The European Union states are:

- Austria
- Belgium
- Bulgaria
- Cyprus
- The Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- United Kingdom

27.3 The other EEA states are:

- Iceland
- Liechtenstein
- Norway