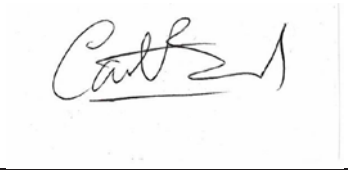
Data Protection & Subject Access Policy

Document Control

Reference Number	**Version** 1.0	**Status** Published	**Sponsor(s)/Author(s)** Andrew Holyoake Principal Information Officer
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			
Group/Persons Consulted: None			
Monitoring Arrangements and Indicators None			
Training/Resource Implications:			
Ratifying Body and Date Ratified		Information Governance Programme Board December 2015	
Date of Issue		February 2016	
Review Date		February 2017	
Contact for Review		Information Governance	
SIRO signature 			

Associated Documentation

Policies
Wiltshire Council controlled documents

- Information Governance Policy
- Information Security Policy
- Password Policy
- Records Management Policy

Legal framework

- Data Protection Act 1998
- Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002
- Human Rights Act 1998
- Criminal Justice and Immigration Act 2008

Contents

1. Introduction

Wiltshire Council holds and processes information about its employees, clients, and other individuals for various purposes (for example, the effective provision of healthcare services, to operate the payroll, and to enable correspondence and communications).

To comply with the Data Protection Act 1998 (the DPA), information must be collected and used fairly, stored safely securely disposed of, and not disclosed to any unauthorised person. The DPA applies to both manual and electronically held data.

The policy applies to all personal information in the council. Non-compliance with this policy may result in disciplinary action.

2. Scope of Policy

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

3. Summary of Aims

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.

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

- Observe fully conditions regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is used;
- 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;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Ensure that the rights of people about whom information is held can be fully exercised under the Act. (These include: the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is shown to be inaccurate information.);

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

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

4. Notification to the Information Commissioner

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

Notification monitoring within the council is carried out by the Information Governance Manager or the Senior Information Governance Lead.

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).

5. Council staff with Data Protection responsibilities

All queries about this council policy should be directed to the Data Protection Lead. Requests for access to social care client's confidential records should be addressed to the Corporate Information Team.

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

See also Section14 Right of Access to Personal Data for more details.

6. Data Protection Principles

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

- Be processed fairly and lawfully and shall not be processed unless certain conditions are met;
- Be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes;
- Be adequate, relevant and not excessive for those purposes;
- Be accurate and kept up to date;
- Not be kept for longer than is necessary for those purposes;
- Be processed in accordance with the data subject's rights under the 1998 Act;
- Be the subject of appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction;

- Not be transferred to a country outside the European Economic Area, unless that country or territory has equivalent levels of protection for personal data.

See Section12 Disclosure outside of the United Kingdom (UK) or European Economic Area (EEA) for more details.

7. Processing

"Processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- Organisation, adaptation or alteration of the information or data;
- Disclosure of the information or data by transmission, dissemination or otherwise making available, or
- Alignment, combination, blocking, erasure or destruction of the information or data.

8. Privacy Notices

Sometimes called a Fair Processing Notice, any collection of personal data must satisfy the requirements of the fair processing condition set out in the first Data Protection Principle.

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

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

This particularly applies to client consent forms: it may be that current forms need to be amended to include a statement about data protection.

The purpose of a Privacy Notice is to explain to the individual:

- The identity of the organisation collecting his or her data;
- How the personal information which is provided will be used;
- Any other information which the individual should be told in order to ensure the processing of his or her information is fair, for example:
    - A description of any other organisations the information may be shared with or disclosed to; whether the information will be transferred outside the UK;
    - The fact that the individual can object to the use of his or her information for marketing;

- The fact that an individual can obtain a copy of his or her information.

Wiltshire Council will ensure that the Privacy Notice is in a prominent position whenever used.

An example form of words for a Privacy Notice might be:

Your personal data will be used only in accordance with the Wiltshire Council notification under the Data Protection Act 1998. The council will not disclose any personal information to any other third parties, without your express consent except where there is a legal justification or required by law.

It is also good practice to include a brief description of what council function the data collection will support.

9. Responsibilities of Individual Data Users

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:

- The requirements of the Data Protection Act 1998 (including the Data Protection Principles);
- The council's Data Protection Policy, including any procedures and guidelines which may be issued from time to time.

A breach of the Data Protection Act and/or the council's Data Protection Policy may result in disciplinary action.

Consideration should be given towards contacting the Principal Information Officer for data protection advice concerning the following:

- When developing a new computer system for processing personal data - it may also be necessary to comply with the council's Database Management Policy and Privacy Impact Assessment Policy;
- 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 Database Management Policy;
- When creating a new manual filing system containing personal data;
- When using an existing manual filing system containing personal data for a new purpose.

Contractors and Data Processors

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.

10. Accuracy of Data

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

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

The council cannot be held responsible for any errors unless the member of staff has informed the council about them.

11. Sensitive Personal Data

a) The council will process "sensitive personal data" relating to staff, clients, contractors and other individuals. This sensitive personal data may include information which has incidentally come into the possession of the council. This type of information will not be routinely sought by the council.

b) In exceptional circumstances, the council may need to process information regarding criminal convictions or alleged offences in connection, for example, with any disciplinary proceedings or other legal obligations.

c) 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 one of the limited exemptions provided in the Data Protection Act 1998 applies (such as to perform a legal duty regarding employees or to protect the data subject's or a third party's vital interests).

12. Data Security and Disclosure

All staffs 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, and that every reasonable effort will be made to see that data is not disclosed accidentally.

Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct. If in any doubt, consult the Information Governance Manager, Senior Information Governance Lead, or Human Resources. Personal data must be kept securely and examples of how this may be done will include:

Keeping the data locked in a 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

Any other appropriate security measures which are detailed in the council IM&T Security Policies.

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.

13. Data Subjects' Consent

Where appropriate the council will seek consent from data subjects to process their personal information.

14. Right of Access to Personal Data

All individuals have the right under the DPA 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 incorrect.

14.1 Individual's Right of Access to Social Care Records

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

Any inaccuracies in data disclosed 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.

The council will seek to respond to the request for access to personal data within 40 calendar days (including bank holidays and weekends) of the request, subject to any applicable exemptions.

14.2 Access to Third Party Personal Data by Elected Representatives

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 may be provided without the council receiving explicit consent from the data subject in question.

15. CCTV

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.

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 where a crime needs to be investigated, but it would not be considered appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet.

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

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

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

16. Email

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

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

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

The council may, from time to time, need to transfer personal data to countries or territories outside of the UK or EEA (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. For example, the names and contact details of members of staff at the council on a website may constitute a transfer of personal data worldwide.

If an individual wishes to raise an objection to this disclosure, then written notice should be given to the council's Principal Information Officer.

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 UK or EEA to a country or territory which

does not ensure an adequate level of protection for the rights and freedoms of data subjects.

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.

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.

18. Retention of Data

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.

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 Management of Records, Section 46, Freedom of Information Act (2000) and the relevant legislation.

All data retention will comply with the 5th Principle of the Data Protection Act 1998.

19. Training

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

20. Appendix A - EEA Countries

The 8th Principle of the Data Protection Act 1998 prohibits the transfer of personal information to countries or territories outside the European Economic Area (EEA).

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

The other EEA states are:
Iceland
Liechtenstein
Norway