Data Protection Policy

January 2020

Document Version	2.3
Document Status	Published
Owner Name	Caroline Parker
Owner Job Title	Information Services Manager
Document ref.	
Approval Date	08/01/2020
Review Date	08/01/2021

Data Protection Policy

Document Control and Information

Status	Approval Date	Review Date
Published	08/01/2020	08/01/2021

Document Owner's Name	Job Title
Caroline Parker	Information Services Manager

Do not alter, copy, publish or distribute without the approval of the Document Owner

This instruction applies to:-

All personal data for which Oxfordshire County Council is the Data Controller, regardless of format, media or location. Where the council is a Data Processor on behalf of another Date Controller, this policy will apply only in so far as it meets the legal obligations of the council. For specific actions as Data Processor, the contract or Information Sharing Agreement with the Data Controller will apply

This includes all temporary and permanent council staff, contractors, staff working under contract for external agencies commissioned by the council, volunteers and Councillors.

For Action by

As above.

For Information

As above.

Revision History

Version	Date	Author / Reviewer	Notes
2.3	08/01/2020	Information Management Team	Annual review
2.2	08/01/2019	Information Management Team	Annual review
2.1	04/06/2018	Information Management Team	Update for GDPR and DPA 2018
2.0	26/10/2017	Information Management Team	Review
1.0	08/2014	Legal Services	Review and update

Distribution and/or Publication

	Location	Date
All Staff	OCC Intranet	08/01/2020

Contents

1. Policy Statement

Oxfordshire County Council collects, processes, stores and disposes of personal data in accordance with the requirements of the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA2018) and any other relevant legislation that governs the use of personal data.

2. Purpose

Council staff, contractors, Councillors and other specified third parties are required to have access to personal data held by the council in the performance of their duties.

This policy describes the council's position on meeting its statutory requirements for collecting, processing, storing and disposing of personal data.

3. Scope

This policy covers all personal data for which Oxfordshire County Council is the Data Controller, regardless of format, media or location.

Where the council is a Data Processor on behalf of another Data Controller, this policy applies only in so far as it meets the legal obligations of the council. For specific actions as Data Processor, the contract or Information Sharing Agreement with the Data Controller will apply.

The policy applies to all temporary and permanent council staff, contractors, staff working under contract for external agencies commissioned by the council, volunteers and Councillors.

4. Policy Compliance

Failure to comply with this policy may lead to disciplinary action. In the case of Council employees this will be in accordance with the agreed disciplinary procedures and Officers Code of Conduct; for elected members it will be in accordance with the Code of Conduct for Members. For other groups the equivalent procedures and standards will apply.

It should also be noted that any information - including emails and attachments - may need to be disclosed under the GDPR and DPA2018, or the Freedom of Information Act 2000.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager.

5. Roles and Responsibilities

All users are required to accept and abide by the requirements of this policy and any associated procedures.

All managers are responsible for ensuring their staff read and abide by this policy and any associated policies and procedures.

6. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Information Services Manager.

7. Data Protection Principles

There are six principles of data protection under the GDPR and DPA2018. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial 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; 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');

(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; 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 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');

(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 addition, there is a requirement that 'The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')'.

There is a further requirement to be able to withdraw consent.

8. Data Protection Requirements

To meet the requirements of the principles above and any other obligations under the GDPR and DPA2018, the council will ensure the following:

1. Renew its entry of the Register of Notifications held by the Information Commissioner's Office
2. Maintain a register of particulars about the types of personal data the council holds, purposes for which it is held and used and types of organisations to which personal data may be disclosed
3. Appoint a Data Protection Officer and officers with specific responsibility for data protection in the council
4. Any forms used to collect data will contain a privacy notice to inform the data subject of the reasons for collecting the personal information and the intended uses
5. Any personal information that has been collected will be used only for the purposes for which it was collected
6. Data subjects (individuals to whom the personal information relates) can exercise their rights under the Act, including the right
    a. To be informed that their personal information is being processed
    b. Of access to their personal information
    c. To correct, rectify, block or erase information that is regarded as wrong
    d. To restrict processing
    e. To data portability
    f. Further rights related to automated decision making.
7. Personal data will only be disclosed to third parties when it is fair and lawful to do so in accordance with the legislation and in compliance with the council's Information Sharing Agreements
8. Information Sharing Agreements are designed to set out the parameters under which formal data sharing can take place simply, safely and securely.
9. Special categories of personal data will only be processed in accordance with Articles 9 and / or 10 of the GDPR. Special categories means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
10. Procedures are in place to check the accuracy of personal data collected, retained and disclosed
11. Review the time that personal information is retained or stored to ensure that it is erased at the appropriate time
12. All officers who hold or process personal information will receive appropriate training in order to comply with the Act

13. Audit compliance with this policy and the Act and any incidents involving breaches of this policy or the Act are recorded, analysed and disciplinary action taken as appropriate
14. This policy is reviewed regularly and updated when necessary.

9. Data Protection Roles

There are different roles involved with the assurance process. Each role requires specialist skills and may require formal training.

Caldicott Guardian

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and social care information and making sure it is used properly.

All NHS organisations and local authorities which provide social services must have a Caldicott Guardian.

The Caldicott Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information.

The Caldicott Guardian has a strategic role, which involves representing and championing issues related to information sharing at senior management team level.

Data Protection Officer (DPO)

The council is required to appoint a Data Protection Officer (DPO), to provide legal support regarding compliance with the legislation.

The DPO role is an independent one, taking formal responsibility for data protection across the organisation and is accountable to the Information Commissioner's Office and responsible to the public.

A DPO must report to the highest management level within an organisation, and should have the professional experience and knowledge of data protection law.

The DPO has the responsibility to:

- inform and advise the organisation and its employees about their obligations to comply with DPA2018 and GDPR and other data legislation;
- monitor compliance with DPA2018 and GDPR and other data legislation, including managing internal data protection activities, advising on data protection impact assessments, ensuring staff are trained and conducting internal audits.

Senior Information Risk Owner (SIRO)

The SIRO is a senior member of the organisation with overall responsibility for the organisation's information risk policy(s) and information risk management strategy. The SIRO is accountable and responsible for:

- information risk across the organisation
- the risk profile of the organisation
- identifying all associated risks

- making sure that appropriate mitigations are in place so that the risks can be removed, reduced or tolerated.

The SIRO also ensures that everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately.

Further Information

The Information Commissioner's Office (ICO) is the independent authority set up to monitor compliance with the Act. It also issues guidance and good practice notes. The ICO's website address is https://ico.org.uk/

The ICO can consider complaints about an organisation's failure to comply with the Act following the initial reply from that organisation. Where appropriate, Oxfordshire County Council will consider complaints using the Corporate Complaints Procedure, however it may refer the complainant directly to the ICO.