Oakford Parish Council

Data Protection Policy 2026

Adopted by the Council 9th March 2026

Review date: March 2028

This policy has been reviewed and updated to ensure compliance with the Data Protection Act 2018, UK GDPR, and ICO guidance as of 2026.

Contents

1. Aims

The Council aims to ensure that all personal data collected about staff, councillors, members of the public, contractors and other individuals is collected, stored and processed in accordance with the Data Protection Act 2018 (DPA 2018) 2018 and the United Kingdom General Data Protection Regulations (UK GDPR) 2021.
This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the Data Protection Act 2018, the provisions of the UK GDPR and is based on guidance issued by the Information Commissioner's Office (ICO) who are the supervisory authority for data protection in England.

3. Key terms

Terminology used within this policy is defined below:

Personal Data – Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Sensitive Personal Data – Data such as:

- Contact details
- Racial or ethnic origin
- Political opinions
- Religious beliefs, or beliefs of a similar nature
- Where a person is a member of a trade union
- Physical and mental health
- Sexual orientation
- Whether a person has committed, an offence
- Criminal convictions

Processing – any activity that involves the use of Personal Data. It includes obtaining, recording or holding data or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Data subject – The person whose Personal Data is held or processed

Data controller – A person or organisation that determines the purposes for which, and the way, Personal Data is processed. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Controller of all Personal Data relating to the Trust.

Data processor – A person, other than an employee of the data controller, who processes the data on behalf of the Data Controller

4. The Data Controller

The Council collects personal data relating to staff, councillors, suppliers and others, and therefore is a data controller. The Council delegates the responsibility of data control to the Clerk.
The Council is registered as a data controller with the ICO and this registration is renewed annually.

5. Data protection principles

The Data Protection Act (DPA) had eight data protection principles, or rules, for good data handling. Under GDPR, there are six rules being:-
Data shall be processed fairly, lawfully and in a transparent way
Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data that is collected shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Data shall be accurate and, where necessary, kept up to date
Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for which the Personal Data is processed
Data shall be processed in a manner that ensures appropriate security of the Personal Data
Accountability is one of the data protection principles. You are responsible for complying with the UK GDPR and need to put in place appropriate technical
and organisational measures to meet the requirements of accountability.
The Council shall always adhere to these rules.

6. Roles and responsibilities

The Council has overall responsibility for ensuring that it complies with its obligations under the DPA. Day-to-day responsibility rests with the Clerk who will ensure that any other staff are aware of their data protection obligations and oversee any queries relating to the storing or processing of Personal Data.
Members of staff are responsible for ensuring that they collect and store Personal Data in accordance with this policy and other related policies and procedures.

Staff
We process data relating to those we employ to work for the Council. The purpose of processing this data is to assist in the running of the Council, including to:

Enable individuals to be paid

Staff Personal Data includes, but is not limited to, information such as:

Contact details
National Insurance Number
Qualifications
Salary information
Absence data
Personal characteristics, including ethnic groups, nationality, marital status and religion
Medical information
Outcome of any disciplinary procedures
We will retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected or in accordance with legislative requirements. We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as HMRC.

7. Lawfulness, Fairness And Transparency

Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

The Council will only collect, process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts its actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that the Council Process Personal Data fairly and without adversely affecting the Data Subject.

8. Consent

Data Subjects consent to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing.

A Data Subject is able to withdraw Consent to Processing at any time.

We will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and Privacy Guidelines, so that we can demonstrate compliance with Consent requirements.

9. Transparency (Notifying Data Subjects)

The UK GDPR requires a Controller to provide detailed, specific information to a Data Subject depending on whether the information was collected directly from the Data Subject or from elsewhere. The information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from a Data Subject, including for HR or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, and how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which

must be presented when the Data Subject first provides the Personal Data. The DPO can be contacted at westbucklandclerk@gmail.com

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

10. Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

We will not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

11. Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

We will ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Trust's data retention guidelines.

12. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

13. Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. The Council will maintain retention policies and procedures to ensure Personal Data is deleted after an appropriate time, unless a law requires that data to be kept for a minimum time. We will not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Council will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Council's applicable records retention schedules and policies. This includes requiring third parties to applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable. We will ensure Data Subjects are provided with

information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

14. Security Integrity and Confidentiality

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage. We will develop, implement and maintain safeguards appropriate to the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable). We will follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction.

15. Reporting a Personal Data Breach

The UK GDPR requires Controllers to notify any Personal Data Breach to the ICO and, in certain instances, the Data Subject. We have put in place procedures to deal with any suspected personal data breach and will notify the data subject or any applicable regulator where we are legally required to do so.

16. Transfer Limitation

The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

Data Subject's Rights and Requests

A data subject has rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw consent to processing at any time
- receive certain information about the Controller's processing activities
- request access to their Personal Data that we hold. Requests may be refused if they are manifestly unfounded or excessive, for example, where threats have been made against employees or offensive language used
- prevent our use of their Personal Data for direct marketing purposes
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data
- restrict processing in specific circumstances
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest
- request a copy of an agreement under which Personal Data is transferred outside of the UK
- object to decisions based solely on automated processing, including profiling (ADM);
- prevent processing that is likely to cause damage or distress to the data subject or anyone else

- be notified of a Personal Data breach which is likely to result in high risk to their rights and freedoms
- make a complaint to the supervisory authority
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

We will verify the identity of an individual requesting data under any of the rights listed above.

17. Accountability

The Controller must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

18. Record Keeping

The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

We will keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum:

- the name and contact details of the Controller and the DPO; and
- clear descriptions of:
  - the Personal Data types;
  - the Data Subject types;
  - the Processing activities;
  - the Processing purposes;
  - the third-party recipients of the Personal Data;
  - the Personal Data storage locations;
  - the Personal Data transfers;
  - the Personal Data's retention period; and
  - the security measures in place.

To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

19. Storage of records

Records are stored in accordance with the Trust's Records Retention Policy and Schedule, which follows requirements published by the Records Management Society and is updated as new guidance is issued. Paper-based records and portable electronic devices containing personal information are kept securely under lock and key when not in use, and confidential papers must never be left on desks, staffroom tables, or noticeboards where general access is possible. When personal information needs to be taken off-site in paper or electronic form, staff must comply with Data Management Procedures. Passwords

must be at least 12 characters long, include letters, numbers, and symbols, and be changed regularly. All portable devices and removable media are protected with encryption software, and staff are prohibited from using personal devices or USBs.

20. Disposal of records

Records are disposed of in accordance with the timeline stated in the Trust's Records Retention Policy and Schedule which complies with legislation and statutory requirements and in accordance with guidance published by the Records Management Society.

Personal information that is no longer needed is disposed of securely. All personal information is shredded or placed in document disposal sacks in the academy offices, and electronic files are overwritten. We may also use an outside company to safely dispose of electronic records.

21. Photos and Videos

As part of our council activities, we may take photographs and record images of individuals.

We will obtain written consent from individual for photographs and videos taken for communication, marketing and promotional materials.

Uses may include:

- Newsletters, etc.
- Outside of the council by external agencies such as newspapers
- Online on our website

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will where practical, delete the photograph or video and not distribute it further.

22. Training and Audit

We are required to ensure all members of staff have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

Data protection will also form part of continuing professional development, where changes to legislation or the Council's processes make it necessary.

23. Responding to Data Subject Access Requests

For exact legal obligations and exemptions applicable in the UK, refer to the Information Commissioner's Office (ICO) Guide to Subject Access. **[1, 2, 3, 4]**