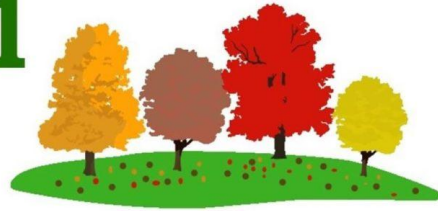


Sunningwell

Parish Council



Subject Access Requests Policy

[Adopted April 30th 2026 Minute Ref 58/26](#)

Introduction

Individuals, also known as data subjects, have the right to access personal data held on them by Sunningwell Parish Council (“the Parish Council”).

Personal Data is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the personal data alone or in conjunction with any other personal data. The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA) and other legislation relating to personal data and rights such as the Human Rights Act 1998.

Further details are set out in the General Privacy Notice, which is available on the Parish Council’s website or from the Parish Council office.

This policy advises of the internal process on handling of Subject Access Requests (SARs) and includes information on:

- Responsibilities
- Timing
- Changes to data; and
- Handling requests for rectification, erasure, or restriction of processing.

The Parish Council will always ensure that personal data is easily accessible, to enable a timely response to SARs. Where this is not reasonably possible, the Parish Council [l](#)

Upon receipt of a Subject Access Request (SAR)

a) Requests must be made in writing but may be submitted electronically (email) or in hard copy. It will be verified that the Parish Council is a Data Controller of the data subject’s personal data.

Once verified, the Data Subject will be informed who at the Parish Council to contact regarding the handling of their SAR. This will normally be the Clerk who has been appointed as the Data Information Officer under the Parish Council’s Data Protection Policy.

b) The identity of the Data Subject will be verified and, if needed, any further evidence on the identity of the Data Subject may be requested. Where identity cannot be verified, the Parish Council will pause the statutory timeframe until adequate evidence is provided.

c) The SAR will be verified. Is it sufficiently substantiated and is it clear to the Data Controller what personal data is requested? If not, additional information will be requested. The Parish Council may ask the requester to narrow the scope where the request is broad but will not require narrowing as a condition of compliance.

d) Requests will be verified to check if they are unfounded or excessive (in particular because of their repetitive character). If they are, the Parish Council may refuse to act on the request or charge a reasonable fee. Any decision to refuse or charge a fee will be documented with clear justification.

e) Receipt of the SAR will be promptly acknowledged, and the data subject will be informed of any costs involved in the processing of the SAR. The acknowledgement will also confirm the expected response date.

f) Whether the Parish Council processes the data requested, will be verified. If the Parish Council does not process any data, the Data Subject will be informed accordingly. At all times, the internal SAR policy will be followed, and progress may be monitored. A written record of searches conducted will be maintained.

g) Data will not be changed because of the SAR. Routine changes, as part of the processing activities concerned, may be permitted. Any changes made during the SAR period will be logged to demonstrate they were not made to avoid disclosure.

h) The data requested will be verified to establish if it involves data on other data subjects. This data will be filtered before the requested data is supplied to the Data Subject. If data cannot be filtered, other Data Subjects will be contacted to give consent to the supply of their data as part of the SAR. If consent is not obtained, the Parish Council will apply the appropriate exemptions and redact third-party data where required.

Responding to a Subject Access Request

a) The Parish Council will respond to a SAR within one calendar month after receipt of the request. The clock starts from the day after receipt of the request, or after identity has been verified:

If more time is needed to respond to complex requests, an extension of another two months is permissible, and this will be communicated to the Data Subject in a timely manner within the first month.

If the Parish Council cannot provide the information requested, it will inform the Data Subject on this decision without delay and, at the latest, within one calendar month of receipt of the request. If a request is refused, a written explanation and information about how to complain will be provided. The Parish Council will also record the reasons for refusal internally.

b) If a SAR is submitted in electronic form, any personal data will be preferably provided by electronic means as well. Secure transfer methods will be used, and password protection will be applied where appropriate.

c) If data on the Data Subject is processed, the Parish Council will ensure, as a minimum, the following information in the SAR response:

i. the purposes of the processing.

ii. the categories of personal data concerned.

iii. the recipients or categories of recipients to whom personal data has been or will be disclosed (in particular, to third countries or international organisations), including details of any appropriate safeguards for international transfers, such as Binding Corporate Rules approved by the Information Commissioner's Office (ICO), or the use of the UK International Data Transfer Agreement (IDTA) or UK Addendum to the EU Standard Contractual Clauses, where applicable^[1];iv. where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period.

v. the existence of the right to request rectification or erasure of personal data, or restriction of processing of personal data concerning the Data Subject or to object to such processing.

vi. the right to lodge a complaint with the Information Commissioners Office (the ICO).

vii. if the data has not been collected from the Data Subject: the source of such data.

viii. the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject.

d) the Parish Council will provide a copy of the personal data undergoing processing. Where providing a copy would adversely affect the rights of others, appropriate redactions will be applied.

Implementing the Subject Access Requests Policy

1. On receipt of a SAR, it must be forwarded immediately to the Finance Working Group who will decide whether a valid request has been made under the Data Protection legislation. A central log of all SARs will be maintained, including dates, actions taken, and outcomes.
- 2.
3. The Data Controller must ensure the request has been received in writing, where a Data Subject is asking for sufficiently well-defined personal data held by the Parish Council,

relating to the Data Subject. What personal data is needed will be clarified with the requestor, who must supply their address and valid evidence to prove their identity. The Parish Council accepts the following forms of identification:

- Current UK/EEA Passport
- UK Photocard Driving Licence (Full or Provisional)
- Firearms Licence/Shotgun Certificate
- EEA National Identity Card
- Full UK Paper Driving Licence
- State Benefits Entitlement Document*
- State Pension Entitlement Document*
- HMRC Tax Credit Document*
- Local Authority Benefit Document*
- State/Local Authority Educational Grant Document*
- HMRC Tax Notification Document
- Disabled Driver's Pass
- Financial Statement issued by bank, building society or credit card company+
- Judiciary Document such as a Notice of Hearing, Summons or Court Order
- Utility bill for supply of gas, electric, water or telephone landline+
- Most recent Mortgage Statement
- Most recent Parish Council Tax Bill/Demand or Statement
- Tenancy Agreement
- Building Society Passbook which shows a transaction in the last 3 months and your address

(*These documents must be dated in the past 12 months;

+These documents must be dated in the past 3 months)

All Parish Councillors and staff, who receive from the Data Controller, a request to locate and supply personal data relating to a SAR must make a full exhaustive search of the records to which they have access. Parish Councillor and staff must confirm in writing that searches have been completed.

3. All the personal data that has been requested must be provided unless an exemption applies. (This will involve a search of emails/recoverable emails, mobile phone texts, social media posts, word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records

in relevant filing systems). The Parish Council will ensure that Councillors and staff understand their obligation to search all locations where personal data may reasonably be held.

4. A response must be provided within one calendar month after accepting the request as valid.
5. The Parish Council must provide, where necessary, an explanation with the personal data in an “intelligible form”, which will include explaining any codes, acronyms, and complex terms. The personal data will be supplied in a permanent form except where the requestor agrees or where it is impossible or would involve undue effort. Agreement may be sought with the requestor that they will view the personal data on screen or inspect files on Parish Council premises.
6. Any exempt personal data will be redacted from the released documents with an explanation why that personal data is being withheld. Redaction will be conducted using secure methods with an audit trail.
7. SARs will be undertaken free of charge to the requestor unless the legislation permits reasonable fees to be charged. Fees will be applied only where allowed by Article 12(5) of the UK GDPR. Any fees charged will be communicated in writing before processing begins.
8. The Clerk and HR Working Group must ensure that all staff are aware of and follow this guidance.
9. Where a requestor is not satisfied with a response to a SAR, the Parish Council must manage this as a complaint under the Parish Council’s Complaints Policy. If unsatisfied, individuals can escalate their complaint to the Information Commissioner’s Office

[1] Binding Corporate Rules (BCRs) are internal data protection policies adopted by multinational organisations to allow the lawful transfer of personal data outside the UK. BCRs must be approved by the Information Commissioner’s Office (ICO) in the UK and are subject to ongoing oversight. Separate approval is required for transfers out of the EU.

UK International Data Transfer Agreement (IDTA) and the UK Addendum to the EU Standard Contractual Clauses (SCCs) are legal tools issued by the UK Government for organisations to ensure appropriate safeguards when transferring personal data to countries not covered by a UK adequacy decision. These replace the use of the EU SCCs for UK-based data transfers.

If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details at the top of this privacy notice.

If you remain unhappy with how we’ve used your data after raising a complaint with us, you can also complain to the ICO.

The ICO’s address:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Helpline number: 0303 123 1113

Website: <https://www.ico.org.uk/make-a-complaint>