

St Paul's Church, Oadby.

Data Protection Complaints Procedure

The Church's Data Protection Officer (DPO) is Graham Neville 07931726661
graham.neville@stpaulsoadby.org

This procedure ensures compliance with UK data protection law (including the Data Protection Act 2018 and the Data (Use and Access) Act) and provides a clear method for individuals to raise concerns about how their personal data is handled. It applies to all employees, contractors, service users, and any third party acting on someone's behalf.

1. Scope

This complaints procedure covers:

- Alleged breaches of data protection law (e.g., unlawful collection, processing, storage, or sharing of data)
- Failure to comply with individual rights (access, rectification, erasure, objection, restriction of processing, portability)
- Complaints raised by third parties authorised to act on behalf of the data subject

2. Methods for Raising a Complaint

To exercise all relevant rights or queries of complaints please in the first instance contact the Data Protection Officer at graham.neville@stpaulsoadby.org Tel : 07931 726661. Or Revd Steve Bailey: rector@stpaulsoadby.org Tel: 07349 959803

Complaints may be submitted through multiple channels, including:

- **Email:** office@stpaulsoadby.org
- **Postal mail:** Church Administrator, St Paul's Church, Hamble Road, Oadby, Leicester, LE2 4NX
- **In person / by phone:** Any employee can accept a complaint and forward it to the Data Protection Officer (DPO)

The complainant may choose their preferred method. The organisation must provide information about how to complain in privacy notices and communications from the point of data collection onward.

3. Acknowledgement

- The DPO or designated complaints handler must **acknowledge receipt within 30 calendar days** of receiving the complaint.
- Acknowledgement should confirm the complaint has been received, the expected timeline, and a point of contact.
- If submitted outside business hours, the acknowledgment period begins the next working day

4. Investigation

- Investigations must start **without undue delay** following receipt of the complaint.
- Relevant staff, data processors, and joint controllers should cooperate and provide information necessary for the investigation.
- The identity of the complainant should be verified early in the process if there is any doubt, using proportionate means (e.g., photo ID, signed authority for third-party complaints).

5. Communication During Investigation

- Complainants must be kept informed of progress, including expected timelines for resolution.

- Any requests for additional information from the complainant should be made **promptly and proportionately**.
- A record must be kept of all communications, actions taken, and decisions made.

6. Outcome and Response

- The organisation must provide a **clear and comprehensive outcome** to the complainant without unreasonable delay.
- The response should include:
 - Explanation of how the complaint was investigated.
 - Details of any remedial actions taken or reasons no further action was required.
 - Reference to the complainant's right to escalate to the **Information Commissioner's Office (ICO)** if they remain unsatisfied.
- Outcomes may be communicated in writing, email, or verbally (for straightforward cases), documented for auditing purposes.

7. Lessons Learned and Review

- After completing the complaint process, the organisation should:
 - Review the cause of the complaint.
 - Identify process or policy improvements to prevent recurrence.
 - Update staff training as necessary.
 - Maintain anonymised records of complaints and trends for internal review.

8. Escalation to the ICO

If the complainant is not satisfied with the resolution or the process, they may contact the **ICO**:

- **Email:** icocasework@ico.org.uk
 - **Post:** Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
 - **Phone:** 0303 123 1113
- Full details: <https://ico.org.uk/make-a-complaint/>

9. Responsibilities

- **Data Protection Officer (DPO):** Overall responsibility for investigating complaints and liaising with complainants.
- **Line Managers / Staff:** Identify, record, and escalate data protection complaints promptly.
- **Joint Controllers / Processors:** Cooperate with investigations and ensure compliance as per contractual agreements.

10. Documentation Requirements

- Record receipt, investigation steps, communications, outcome, and lessons learned for each complaint.
- Track recurring themes and trends to inform organisational risk management and compliance audits.

This procedure ensures transparency, accountability, and adherence to legal obligations under UK data protection law, enhancing trust and regulatory compliance.

Source(s):

1. <https://www.gov.uk/government/publications/data-protection-complaints-process/data-protection-complaints-process>
2. <https://ico.org.uk/make-a-complaint/>
3. <https://dpnetwork.org.uk/data-protection-complaints-new-requirements/>