Data Protection Policy and Privacy notice

Data Protection Policy

The church needs to gather and use certain personal information about individuals. This includes volunteers.

Anyone working on the church's behalf (including volunteers) have responsibilities to ensure compliancy with the provisions under the Data Protection Act 2018 (DPA 2018), and therefore must ensure that:

- personal data is processed fairly, lawfully and in a transparent manner;
- personal information must have a lawful basis for processing;
- data is obtained for specified and lawful purposes and not further processed in a manner that is incompatible with those purposes;
- the data is adequate, relevant and not excessive;
- the data is accurate and where necessary kept up to date;
- data must not be kept for longer than necessary and in line with the retention policy; and
- data is kept secure.

Volunteers must not disclose personal data outside the church's procedures, or use personal data held on others for their own purposes. Any suspected or known data breach must lead to immediate action under the **Data Breach Procedure**.

Volunteers have a right to access information that the church may hold on them. If a volunteer wants to see their personal data, they should speak to the volunteer co-ordinator.

If the church is unable or unwilling to agree to the request, a volunteer could make a Subject Access Request in writing and include:

- full name, address and contact details;
- any information used by the church to identify the volunteer; and
- details of the specific information required and any relevant dates.

A fee for Subject Access Requests may be required if the request is "manifestly unfounded or excessive".

If the church refuses a request, the individual will be informed within one month:

- why the request was refused; and
- of the right to complain to the supervisory authority and to a judicial remedy.

Data Breach Procedure

Volunteers (and staff) have a responsibility to immediately follow these procedures if there is a known or suspected breach of personal data. The approach, subject to individual situations, will generally be:

1. **Breach alert is made or identified** (from whatever source, internal or external)

2. **Data Protection Lead is immediately informed** (Phil Papps; Gay Jacklin in his absence)

3. **Type of breach is recorded** as:

    a. Hacking/electronic security breach
    b. Office physical security breach
    c. Lost data (known or suspected)
    d. Stolen data – outside office (known or suspected)
    e. Disclosure without authority
    f. Other

4. **Response actions by Data Protection Lead**:

    a. Investigate what data is missing and who is affected.
    b. What are the security implications (e.g. is other data now potentially at risk)?
    c. What measures must be immediately taken to reduce the risks and make other data secure?
    d. Determine what and how the breach is communicated to those potentially affected or who need to know.
    e. Alert Trustees and agree actions as appropriate.
    f. Determine if the breach is reportable to the ICO. If so, report within the 72 hour timescale (unless it is unlikely to result in a risk to the rights/freedoms of the individual).
    g. Alert church insurers as appropriate.
    h. Ensure all of the above is documented.

5. **Remedial actions**:

    a. Review what happened.
    b. Identify any requirements made by the ICO or our insurers.
    c. Identify changes of practice required or recommended.
    d. Identify changes of security required or recommended.
    e. Invite scrutiny by the appointed Senior Information Risk Owner (Steve Tucker, Trustee) and agree what needs to be communicated and to whom.
    f. Identify any disciplinary action and implement.
    g. Consider at annual review the impact of the breach and the success of any new measures/ changes.