St Giles & St George
Alms and education since 1661

DATA PROTECTION PROCEDURES

1. Subject Access Requests

Any individual who wants to exercise their right to receive a copy of their personal data can do so by making a Subject Access Request, ('SAR') to the Clerk to the Trustees. The request must be made in writing, and the individual must satisfy the clerk of their identity before receiving access to any information.

A SAR must be answered within 40 calendar days of receipt by the charity but we will endeavour to meet any request within 10 working days.

2. Staff/ Director Induction

All new staff member or Directors will be briefed on Data Protection responsibilities. They will be provided with a copy of the charities' Privacy Policy.

All Directors, staff, freelancers and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their roles.

Significant breaches of these policies will be handled under disciplinary procedures.

3. Annual Review of Data Protection

On behalf of the Directors, the Clerk to the Trustees will undertake an annual review of data protection including:

- maintain an audit of the personal data that is held and where it is located;
- review the Legitimate Interests Assessment;
- review the Privacy Policy;
- review the Privacy Notices in the relevant forms;
- ensure that Data Protection training has/is taking place;
- destroy personal data when it no longer needs to be processed;
- report to the Trustees, particularly any actions that need to be taken.

4. Responding to data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

If either of the charities experience a data breach, they will follow these four steps:

Step 1 – Identify the scale of the problem – what data is involved.
Step 2 – Keep a record of all personal data breaches.
Step 3 – Assess whether this poses a risk to people. We will consider the likelihood and severity of the risk to people's rights and freedoms, following the breach. If it is likely there will be a risk, then we will notify the ICO. If it is unlikely, then we will not report. We will use the ICO self-assessment tool.
Step 4 – Report the breach:

- If the breach is serious, then we will report to the ICO within 72 hours.
- If the breach is serious, then we will inform the affected individual.
- All breaches will be reported to the Directors.