

General Data Protection Regulation Policy

1. Purpose of the policy and background to the General Data Protection Regulation (GDPR).

This policy explains to Churches Together in Oxfordshire and the public about GDPR. Personal data must be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures security. This policy includes the requirements of GDPR which apply in the UK from 25th May 2018. The Government having confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement. This policy explains the duties and responsibilities of Churches Together in Oxfordshire and it identifies the means by which Churches Together in Oxfordshire will meet its obligations.

2. Identifying the roles and minimising risk.

GDPR requires that everyone within Churches Together in Oxfordshire must understand the implications of GDPR and that roles and duties must be assigned. Churches Together in Oxfordshire is the data controller and the Enabling Group Secretary is the Data Protection Officer (DPO). It is the DPO's duty to undertake an information audit and to manage the information collected by Churches Together in Oxfordshire, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information.

3. GDPR requirements for care.

GDPR requires continued care by everyone within Churches Together in Oxfordshire, in the sharing of information about individuals, whether as hard copy or electronically. A breach of the regulations could result in Churches Together in Oxfordshire facing a fine from the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as medium risk to Churches Together in Oxfordshire (both financially and reputationally). Such risk can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and Churches Together in Oxfordshire undertaking training in data protection awareness.

4. Data breaches

One of the duties assigned to the DPO is the investigation of any breaches. Personal data breaches should be reported to the DPO for investigation. The DPO will conduct this with the support of Churches Together in Oxfordshire. Investigations must be undertaken within one month of the report of the breach. Procedures are in place to detect, report and investigate a personal data breach. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will also have to notify those concerned directly.

It is unacceptable for staff or officers of Churches Together in Oxfordshire to use IT in any way that may cause problems for Churches Together in Oxfordshire, for example the discussion of internal

Churches Together in Oxfordshire matters on social media sites which could result in reputational damage for Churches Together in Oxfordshire and to individuals.

5. Privacy Notices

Being transparent and providing accessible information to individuals about how Churches Together in Oxfordshire uses personal data is a key element of the Data Protection Act 1998(DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about the data controller and Data Protection Officer, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing a Privacy Notice must be detailed on the Information Audit kept by the council. The council will adopt a privacy notice to use, although some changes could be needed depending on the situation, for example where children are involved. All privacy notices must be verifiable.

6. Information Audit

The DPO must undertake an information audit which details the personal detail held, where it came from, the purpose for holding that information and with whom Churches Together in Oxfordshire will share that information. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when Churches Together in Oxfordshire undertakes a new activity. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

7. Individuals' Rights

GDPR gives individuals rights with some enhancements to those rights already in place: -

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- Right to data portability
- The right to object
- The right not to be subject to automated decision making including profiling.

8. Enhancements to GDPR

8.1. Individuals now have a right to have their personal data erased (sometimes known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge. Data portability refers to the ability to move, copy, or transfer data easily between different computers. If a request is received to delete information, then the DPO must respond to this request within a month. The DPO has the delegated authority from Churches Together in Oxfordshire to delete information. If a request is considered to be manifestly unfounded then the request could be refused. Churches Together in Oxfordshire will be informed of such requests.

8.2. **Children.** There is special protection for the personal data of a child. The age when a child can give their own consent is 13. If Churches Together in Oxfordshire requires consent from young people under 13, Churches Together in Oxfordshire must obtain a parent or guardian's consent in order to process the personal data lawfully. Consent forms for children age 13 plus, must be written in a language that they will understand.

9. Summary

The main actions arising from this policy are:

- A copy of this policy will be available on the Churches Together in Oxfordshire website. The policy will be considered as a core policy of Churches Together in Oxfordshire.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- **Privacy notices must be issued.**
- Churches Together in Oxfordshire will manage the process

This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO.

Churches Together in Oxfordshire are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of Churches Together in Oxfordshire.

Churches Together in Oxfordshire
15th February 2022