UPPER THAMES CIRCUIT – POLICY

DATA PROTECTION POLICY

This policy exists to ensure that the Upper Thames Circuit:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

1. Data protection law

The Data Protection Act 1998 describes how organisations — including the Upper Thames Circuit must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

The General Data Protection Regulation (EU) 2016/679 is applicable from 25.05.2018 and strengthens the 1998 Act by applying a single set of rules across the EU with each member State establishing an independent Supervisory Authority. In particular its regulations require that data is:

- Processed *lawfully, fairly and in a transparent manner* (if we ask for data we should tell the person why it is needed);
- Collected for *specified, explicit and legitimate purposes* and only used for that purpose;
- *Adequate, relevant and limited to what is necessary* (i.e. do not collect data "just in case");

- *Accurate and, where necessary, kept up to date* (someone can ask for their data to be up-dated "without delay");
- Kept in a form which means that once we no longer need the information[1] it can be deleted and no record then exists of that person;
- Processed in a manner that *ensures appropriate security* (including protection against unauthorised or unlawful use and against accidental loss[2], destruction or damage - using appropriate technical or other measures (known as '*integrity and confidentiality'*);

The controller (i.e. the Upper Thames Circuit) shall be responsible for and be able to *demonstrate compliance* ('*accountability'*).

Data may only be held lawfully if at least one of the following applies:

1 the person has given their *consent*;

2 it is necessary to use the data to fulfil a contract;

3 compliance with a legal requirement;

4 to protect someone's life or help them by contacting a relative in case of accident or emergency (*vital interests*);

5 to carry out a task which is in the public interest;

6 *Legitimate Interest* (whereby we could reasonably be expected to do use data to execute certain actions unless it overrides the rights of the person.

For most charitable organisations, usage of data would normally be under 1 or 6 above unless being used for Human Resource purposes in the case of an employee.

2. Policy scope

This policy applies to:

- The Circuit Leadership Team
- Individual Churches within the Upper Thames Circuit
- All employees and volunteers within our churches
- Any contractors, suppliers and other people working on behalf of the Upper Thames Circuit or its churches.

---

[1] Duration is covered in section 7.2.4

[2] For example, RWBMC could state in its new Lettings Process that the Office will never be "let" to minimise the risk of accidental loss of data)

It applies to all data that the Upper Thames Circuit and its churches holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

3. Data protection risks

This policy helps to protect the Upper Thames Circuit and its Churches from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the church or circuit uses data relating to them.
- **Reputational damage.** For instance, the churches or Circuit could suffer if hackers successfully gained access to sensitive data.

4. Responsibilities

Everyone who works for or with the Upper Thames Circuit and its churches has some responsibility for ensuring data is collected, stored and handled appropriately.

Everyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Circuit Meeting** is ultimately responsible for ensuring that meets its legal obligations.
- The **Senior Circuit Steward** will be the Data Protection Officer and is responsible for:
    - Keeping the Circuit Meeting updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies
    - Arranging data protection training and advice for the people covered by this policy.

- Handling data protection questions from staff, employees and anyone else covered by this policy.
- Dealing with requests from individuals to see the data the Circuit holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the Circuit's sensitive data.

The **Senior Circuit Steward** is responsible for working with the Circuit's IT Consultant towards:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the Upper Thames Circuit is considering using to store or process data. For instance, cloud computing services.

5. General guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, ministers can request it from the senior circuit steward and employees can request it from their line managers.
- Ministers, Circuit Stewards and Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the Circuit or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the senior circuit steward if they are unsure about any aspect of data protection.

6. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed via the Senior Circuit Steward to the Circuit's ICT consultant.

The retention of data and the deletion of email chains will be reviewed on an annual basis.

Data will not be kept longer than is necessary to fulfil the purposes for which it is held. Data will only be retained for the period of time for which it is legitimately needed by the Upper Thames and thereafter deleted unless such data must be held for legal purposes. In compliance with this the Circuit will annually consider:

- the current and future value of the information;
- the costs, risks and liabilities associated with retaining the information; and
- the ease or difficulty of making sure it remains accurate and up to date.

In the case of employees pay-roll details will be held for 3 years and personal information for the purposes of references for 5 years after the employee ceased to hold their post.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet** with access limited to named personnel with legitimate need.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data will be stored on an **approved cloud computing services** which will also provide back up protection.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All computers containing data will be protected by **approved security software and a firewall**.

7. Data use

Personal data is of no value to the Upper Thames Circuit unless it can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, staff and employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data held in trust **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT consultant can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees and Circuit Officers **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

8. Data accuracy

The law requires the Upper Thames Circuit to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Unnecessary additional data sets should not be created.
- Data must be **updated as inaccuracies are discovered**.

9. Subject access requests

All individuals who are the subject of personal data held by the Upper Thames Circuit are entitled to:

- Ask **what information** the Circuit holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the Circuit is **meeting its data protection obligations**.

If an individual contacts the Circuit requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Senior Circuit Steward at seniorsteward@upperthamescircuit.org.uk or in writing to the Circuit Administrator at the Circuit Office.

~~Individuals will be charged £10 per subject access request~~. The Administrator under the guidance of the Senior Circuit Steward will aim to provide the relevant data within 14 days.

The Senior Circuit Steward will always verify the identity of anyone making a subject access request before handing over any information.

10. Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the Upper Thames Circuit will disclose requested data. However, the Senior Circuit Steward will ensure the request is legitimate, seeking assistance from the Circuit's legal advisers where necessary.

11.Providing information to employees

The Upper Thames Circuit will ensure that individuals are aware that their data is being processed or retained, and that they understand:

- How the data is being used
- How to exercise their rights
- To these ends, the Circuit has a privacy statement, setting out how data relating to individuals is used by the Circuit as follows

Upper Thames Circuit of the Methodist Church

The Data Protection Act 1998: How we use your information

We process personal data relating to those we employ within the Circuit.
This is for employment purposes to assist in the Circuit's work and/or to enable individuals to be paid.

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. In certain circumstances we may be required to pass on some of this personal data to:

- The Bristol District of the Methodist Church
- The Connexion of the Methodist Church

If you require more information about how we store and use your personal data please ask the Senior Circuit Steward for the Circuit.

If you want to see a copy of information about you that we hold, please contact:

The Senior Circuit Steward: seniorsteward@upperthamescircuit.org.uk

July 2017

Revised and approved 26th September 2017

Amended in the light of the GDPR 5th March 2018