# Appendix 4

## Our data protection responsibilities

Anyone who thinks that they have accidentally breached the policy must contact the Data Protection Trustee immediately so that we can take swift action to try and limit the impact of the breach.

Anyone who breaches the Data Protection Policy may be subject to disciplinary action, and where that individual has breached the policy intentionally, recklessly, or for personal benefit they may also be liable to prosecution or to regulatory action.

Any questions about this policy or any concerns that the policy has not been followed should be referred to the Data Protection Trustee.

### What personal information do we process?

In the course of our work, we may collect and process information (personal data) about many different people (data subjects). This includes data we receive straight from the person it is about, for example, where they complete forms or contact us. We may also receive information about data subjects from other sources including, for example, previous employers.

We process personal data in both electronic and paper form and all this data is protected under data protection law. The personal data we process can include information such as names and contact details, education or employment details and visual images of people.

In some cases, we hold types of information that are called “special categories” of data in the GDPR. This personal data can only be processed under strict conditions.

‘Special categories’ of data (as referred to in the GDPR) includes information about a person’s: racial or ethnic origin; political opinions; religious or similar (e.g. philosophical) beliefs; trade union membership; health (including physical and mental health, and the provision of health care services); criminal proceedings or offences or allegations of offences; genetic data; biometric data; sexual life and sexual orientation.

Other data may also be considered ‘sensitive’ such as bank details but will not be subject to the same legal protection as the types of data listed above.

### Making sure processing is fair and lawful

Processing of personal data will only be fair and lawful when the purpose for the processing meets a legal basis, as listed below, and when the processing is transparent. This means we will provide people with an explanation of how and why we process their personal data at the point we collect data from them, as well as when we collect data about them from other sources.

We will only process personal data when at least one of these legal conditions, as listed in Article 6 of the GDPR, is met:

* the processing is necessary for a contract with the data subject;
* the processing is necessary for us to comply with a legal obligation;
* the processing is necessary to protect someone’s life (this is called “vital interests”);
* the processing is necessary for us to perform a task in the public interest, and the task has a clear basis in law;
* the processing is necessary for legitimate interests pursued by Anytown Baptist Church or another organisation, unless these are overridden by the interests, rights and freedoms of the data subject.
* If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their clear consent.

We will only process ‘special categories’ of personal data when, in addition to the conditions above, one of the extra conditions, as listed in Article 9 of the GDPR, is met. These conditions include, where:

* the processing is necessary for carrying out our obligations under employment and social security and social protection law;
* the processing is necessary for safeguarding the vital interests (in emergency, life or death situations) of an individual and the data subject is incapable of giving consent;
* the processing is carried out in the course of our legitimate activities and only relates to our members or persons we are in regular contact with in connection with our purposes;
* the processing is necessary for pursuing legal claims.

If none of the other legal conditions apply, the processing will only be lawful if the data subject has given their explicit consent. Before deciding which condition should be relied upon, we may refer to the original text of the GDPR as well as any relevant guidance, and seek legal advice as required. If personal data is collected directly from the individual, we will inform them about:

* our identity / contact details and those of the Data Protection Trustee, the reasons for processing, and the legal bases, explaining our legitimate interests and explaining, where relevant, the consequences of not providing data needed for a contract or statutory requirement;
* who we will share the data with;
* if we plan to send the data outside of the European Union;
* how long the data will be stored and the data subjects’ rights.

This information is commonly referred to as a ‘Privacy Notice’ and will be given at the time when the personal data is collected.

If data is collected from another source, rather than directly from the data subject, we will provide the data subject with the information described as above, as well as the categories of the data concerned and the source of that data.

This information will be provided to the individual in writing and no later than one month after we receive the data, unless a legal exemption under the GDPR applies. If we use the data to communicate with the data subject, we will at the latest give them this information at the time of the first communication.

If we plan to pass the data onto someone else outside of Anytown Baptist Church, we will give the data subject this information before we pass on the data, unless a legal exemption to informing the data subject applies.

### When we need consent to process data

Where none of the other legal conditions apply to the processing, and we are required to get consent from the data subject, we will clearly set out what we are asking consent for, including why we are collecting the data and how we plan to use it. Consent will be specific to each process we are requesting consent for and we will only ask for consent when the data subject has a real choice whether or not to provide us with their data. However, consent can be withdrawn at any time and, if withdrawn, the processing will stop. Data subjects will be informed of their right to withdraw consent and it will be as easy to withdraw consent as it is to give consent.

### Processing for specified purposes

We will only process personal data for the specific purposes explained in our privacy notices (as described above) or for other purposes specifically permitted by law. We will explain those other purposes to data subjects in the way described above unless there are lawful reasons for not doing so.

### Data will be adequate, relevant and not excessive

We will only collect and use personal data that is needed for the specific purposes described above (which will normally be explained to the data subjects in privacy notices). We will not collect more than is needed to achieve those purposes. We will not collect any personal data “just in case” we want to process it later.

### Accurate data

We will make sure that personal data held is accurate and, where appropriate, kept up to date. The accuracy of personal data will be checked at the point of collection and at appropriate points later on.

### Keeping data and destroying it

We will not keep personal data longer than is necessary for the purposes it was collected. We will comply with official guidance issued to our sector about retention periods for specific records.

### Security of personal data

We will use appropriate measures to keep personal data secure at all points of the processing. Keeping data secure includes protecting it from unauthorised or unlawful processing, or from accidental loss, destruction or damage.

We will implement security measures that provide a level of security appropriate to the risks involved in the processing. These will include technical and organisational security measures. In assessing what measures are the most appropriate we will take into account the following, and anything else that is relevant:

* the quality of the security measure;
* the costs of implementation;
* the nature, scope, context and purpose of processing;
* the risk (of varying likelihood and severity) to the rights and freedoms of data subjects;
* the risk which could result from a data breach.

Measures may include:

* technical systems security;
* measures to restrict or minimise access to data;
* measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;
* physical security of information and of our premises;
* organisational measures, including policies, procedures, training and audits;
* regular testing and evaluating of the effectiveness of security measures.

### Keeping records of our data processing

To show how we comply with the law we will keep clear records of our processing activities and of the decisions we make concerning personal data (setting out our reasons for those decisions).

### Working with people we process data about (data subjects)

#### Data subjects’ rights

We will process personal data in line with data subjects' rights, including their right to:

* request access to any of their personal data held by us (known as a Subject Access Request);
* ask to have inaccurate personal data changed;
* restrict processing, in certain circumstances;
* object to processing, in certain circumstances as defined by the GDPR, including preventing the use of their data for direct marketing;
* data portability, which means to receive their data, or some of their data, in a format that can be easily used by another person (including the data subject themselves) or organisation;
* not be subject to automated decisions, in certain circumstances as defined by the GDPR; and
* withdraw consent when we are relying on consent to process their data.

If a worker receives any request from a data subject that relates or could relate to their data protection rights, this will be forwarded to our Data Protection Trustee immediately.

We will act on all valid requests as soon as possible, and at the latest within one calendar month, unless we have reason to, and can lawfully extend the timescale. This can be extended by up to two months in some circumstances as defined by the GDPR.

All data subjects’ rights are provided free of charge.

Any information provided to data subjects will be concise and transparent, using clear and plain language.

#### Direct marketing

We will comply with the rules set out in the GDPR, the Privacy and Electronic Communications Regulations (PECR) and any laws which may amend or replace the regulations around direct marketing. This includes, but is not limited to, when we make contact with data subjects by post, email, text message, social media messaging, telephone (both live and recorded calls) and fax.

Direct marketing means the communication (by any means) of any advertising or marketing material which is directed, or addressed, to individuals. “Marketing” does not need to be selling anything or be advertising a commercial product. It includes contact made by organisations to individuals for the purposes of promoting the organisation’s aims.

Any direct marketing material that we send will identify Anytown Baptist Church as the sender and will describe how people can object to receiving similar communications in the future. If a data subject exercises their right to object to direct marketing we will stop the direct marketing as soon as possible.

## Working with other organisations and transferring data

### Sharing information with other organisations

We will only share personal data with other organisations or people when we have a legal basis to do so and if we have informed the data subject about the possibility of the data being shared (in a privacy notice - see Appendix 4), unless legal exemptions apply to informing data subjects about the sharing. Only authorised and properly instructed trustees are allowed to share personal data.

We will keep records of information shared with a third party, which will include recording any exemptions which have been applied, and why they have been applied. We will follow the ICO’s statutory Data Sharing Code of Practice (or any replacement code of practice) when sharing personal data with other data controllers. Legal advice will be sought as required.

### Data processors

Before appointing a contractor, who will process personal data on our behalf (a data processor) we will carry out due diligence checks. The checks are to make sure the data processor will use appropriate technical and organisational measures to ensure the processing will comply with data protection law, including keeping the data secure, and upholding the rights of data subjects. We will only appoint data processors who can provide us with sufficient guarantees that they will do this.

We will only appoint data processors on the basis of a written contract that will require the processor to comply with all relevant legal requirements. We will continue to monitor the data processing, and compliance with the contract, throughout the duration of the contract.

### Transferring personal data outside the European Union (EU)

Personal data will not be transferred (or stored) outside of the European Union unless this is permitted by the GDPR. This includes storage on a “cloud” based service where the servers are located outside the EU.

We will only transfer data outside the EU where it is permitted by one of the conditions for non-EU transfers in the GDPR

## Managing change and risks

### Data protection impact assessments

When we are planning to carry out any data processing which is likely to result in a high risk we will carry out a Data Protection Impact Assessment (DPIA). These include situations when we process data relating to vulnerable people, trawling of data from public profiles, using new technology, and transferring data outside the EU. Any decision not to conduct a DPIA will be recorded.

We may also conduct a DPIA in other cases when we consider it appropriate to do so. If we are unable to mitigate the identified risks such that a high risk remains we will consult with the ICO.

DPIAs will be conducted in conformity with the ICO’s Code of Practice ‘Conducting privacy impact assessments’.

### Dealing with data protection breaches

Where Workers, or contractors working for us, think that this policy has not been followed, or data might have been breached or lost, this will be reported immediately to the Data Protection Trustee.

We will keep records of personal data breaches, even if we do not report them to the ICO.

We will report all data breaches which are likely to result in a risk to any person, to the ICO. Reports will be made to the ICO within 72 hours from when someone in the church becomes aware of the breach.

In situations where a personal data breach causes a high risk to any person, we will (as well as reporting the breach to the ICO), inform data subjects whose information is affected, without undue delay. This can include situations where, for example, bank account details are lost or an email containing sensitive information is sent to the wrong recipient. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.