DATA PROTECTION POLICY

CROWN JESUS MINISTRIES

Importance of Data Protection
The use of personal data is governed by the General Data Protection Regulation ("GDPR"). We take data protection very seriously and understand the impact that data breaches and misuse of data may have on data subjects as well as on our activities. Compliance with this policy is necessary for us to maintain the confidence and trust of those whose personal data we handle.

Who this policy applies to
Everyone, including staff, academy students and volunteers should be aware that they must take care when handling personal data belonging to adults and children.

Purpose of this policy
The purpose of this policy is to give a basic understanding of the data protection laws, our responsibility in respect of data protection practice and your rights and obligations.

What is data?
This is information which:
(a) Is processed by equipment operating automatically, (e.g. computer held information);
(b) Recorded with the intention that it should be processed, (e.g. paper held information which is later put on computer);
(c) Recorded as part of a filing system, (e.g. Registers,

Databases). There are two relevant types of data, personal data

and sensitive data.

What is personal data?
Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Examples of personal data
This can include an individual's name, address, date of birth, contact number, email address, details of family members, photographs, etc.

What is sensitive data?
This means personal data containing information such as:

(a) Racial or ethnic origin
(b) Political opinions
(c) Religious and other similar beliefs
(d) Membership of trade union (which may be relevant in the case of church employees)
(e) Physical or mental health
(f) Sexual life
(g) Criminal record (including alleged offences) and sentence

Rights and Obligations
This Act protects the rights of individuals whose data is held, (known as data subjects) and places obligation on those who hold and process the data. In CJM the Board is legally responsible for data protection. For practical application, the Board has a named member of the Senior Leadership Team.

Data Protection Principles
We will process personal data in accordance with GDPR and good data protection practice.
(a) We will process personal data fairly and lawfully.
(b) Personal data must be obtained for one or more specific lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes. E.g. If information was obtained only for a specific purpose, the data will not be used for other purposes such as upcoming CJM events, except where consent has been sought.
(c) The data must be adequate, relevant and not excessive in relation to the purpose for which it is held.
(d) The personal data must be accurate and where necessary, kept up to date.
(e) Personal data processed for any purpose must not be kept longer than it is necessary for that purpose.
(f) Personal data must be processed in accordance with the rights of the data subjects.
(g) Appropriate technical and organisational measures must be taken to prevent unauthorised or accidental access to personal data.
(h) Personal data must not be transferred outside the EU.

In order to meet these requirements, the following best practice listed below will apply.

Acquisition of Personal Data

- The subjects (or guardians of the subjects) should be told for what purpose(s) the data is being gathered and obtain their explicit consent. In the event that the data will be disclosed to a third party, this must be made known.
- If sensitive data is collected, explicit consent is required, that is consent to hold

the data.

• No more data than necessary should be collected for the purpose(s) declared.

Holding, Safeguarding and Disposal of Personal Data
Retention of Information

• All data such as consent forms, accident forms, or any information on participants should be kept in a secure location, such as a locked filing cabinet.

• Data should not be kept in a person's own home for longer than necessary.

• While in transit, data must not be left unattended i.e. in a car.

• Incident/accident forms must be held securely on CJM premises.

• Data that relates to a one-off event must be securely disposed of at the end of the period or event.

• Data held centrally by CJM and does not pertain to one-off events, should be reviewed annually for storage and destruction.

Who should have access to the information?

• Information should be accessible to a limited team of processors i.e. those gathering, amending, utilising, safeguarding and destroying the information.

• The exception to this, upon consent, is medical information where it is important that all leaders in a supervisory role are aware of a medical condition of a participant or team member in the interest of health and safety.

• Information should not be given to a third party and must only be used for the purpose required.

What about data kept on computers?

• The same rules apply for data kept on computers. Data is confidential and should be kept secure. In order to keep the data protected, it should be held on a system with limited access or varied rights.

How long should records be kept?

• Consent forms, (basic information such as name, date of birth and address) should be kept for up to six years after the person has left the organisation. Thereafter, it should either be destroyed.

• The same applies to information on staff - i.e. it is retained for up to six years after they have left their position.

• Incident/accident forms should be kept for six years for adults, and for children until their 21st birthday. Data for people with a disability of a mental ill health nature should be stored until six years after death.

• All paper held data must subsequently be scanned and held electronically for the duration stipulated above.
This will be reviewed and updated when necessary.

Requests for data
Individuals are entitled to make a request for a copy of the personal data we hold about them. We will endeavour to answer the request promptly and within one month of receipt. Any requests must be passed to Lisa Keys.

Data Breach
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. Any suspected data breaches should be reported immediately to Amanda Mitchell who will log the breach, deal with it and resolve any issues arising out of the breach.

Supporting Documents

In addition to the Data Protection Policy, all staff ,must be familiar with the Data Privacy