GCM DATA PROTECTION POLICY

1. Introduction

This policy sets out how Gloucester City Mission (GCM) will handle personal details and data about its staff, volunteers, trustees, supporters, and clients. To comply with the law, information must be collected and used fairly, stored safely, and not disclosed to any other person unlawfully.

All GCM staff, volunteers, and Trustees must comply with the General Data Protection Principles which are set out in the General Data Protection Regulation 2018 and must ensure that they always follow these principles . Failure to follow the policy can result in disciplinary proceedings.

2. Who is responsible for the Data Protection Policy?

The Trustees of GCM are responsible for the Data Protection Policy. However, the Data Controller and Data Protection Officer are responsible for answering any queries regarding the policy. It is the role of the Data Protection Officer to advise the charity on the rules needed to ensure compliance with data protection laws.

The Designated Data Controller and Data Protection Officer is the Administrator.

3. Summary of the General Data Protection Principles

Data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a manner which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

4. Procedure for Processing Data

The flowchart at the end of this policy details the various avenues personal data flows into, through, and out of GCM. The flow charts also detail where the data came from, who it is shared with, what we do with it, and where it is securely kept.
The categories and details of personal data held are as follows:

Applications/Staff
Names, addresses, telephone numbers, e-mail contact details, recruitment information/application form content;

DBS check details, payroll information and bank account details, sickness records, and next of kin.

Applications/Volunteers
Names, addresses, telephone numbers, e-mail contact details, recruitment information/application form content; DBS check details, and next of kin.

Supporters
Names, addresses, telephone numbers, e-mail contact details, and record of financial giving.

Clients
Names, addresses, telephone numbers, e-mail contact details, relevant medical and benefit information.

In the case of personal details being used in GCM publications, whether by name or photos, written or electronic, permission will always be sought from the data subject.

Certain items of information relating to staff will be made available via searchable directories on the public Website, in order to meet the legitimate needs of those seeking to make contact. Names of those involved in the various ministries of GCM are included in the information given on the Website, together with office telephone numbers and e-mail addresses: no other personal details are released into the public domain.

The key people involved in processing personal data at GCM are as follows:
Administrator (also Data Protection Officer)

- Responsible for the overall processing of personal data, and the processing of the personal data of supporters, staff, volunteers.

Volunteer Coordinator
Responsible for the processing of the personal data of volunteers where the data is processed

Each member of staff or volunteer whose work involves storing personal data must take personal responsibility for its secure storage. Personal data should:

- Be kept in a locked unit.
- If computerised, be password protected, and on a network drive that is regularly backed up.
- If a copy is kept on removable storage media, that media must itself be kept in a locked unit.
- Not be processed or stored off site, at home, or at other remote sites, whether in manual or electronic form, on laptop computers or other personal portable devices, unless there are exceptional circumstances when authority must be obtained by the Designated Data Controller.

Records are kept of any processing of personal data that:

- are not occasional; could result in a risk to the rights and freedoms of individuals;
- involve the processing of special categories of data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sexual life or orientation) or criminal conviction and offence data.

Personal and special categories of data are processed under the lawful basis of Consent. The individual will need to give clear consent for us to process their personal data for a specific purpose. Consent requests include the name of our organisation; the name of any third party controllers who will rely on the consent; why we want the data; what we will do with it; and that individuals can withdraw consent at any time. Individuals are asked to actively opt in and records are kept to

evidence consent.

Should an individual request a change to the personal data we hold, the identity of the individual will be verified using the personal data currently stored and the request will be responded to without delay and within a month of receipt. The request will be managed by the Administrator and passed on for processing to the necessary people using the data processing flowchart.

Should an individual request that their data is erased, the identity of the individual will be verified using the personal data currently stored and the request will be responded to without delay and within a month of receipt. The request will be managed by the Administrator and passed on for processing to the necessary people using the data processing flowchart. GCM ensures that any Disclosure information is disposed of immediately after the retention period has elapsed. Personal data is to be disposed of in the following ways:

- Paper personal data will be permanently destroyed by shredding or incinerating, depending on the sensitivity of the personal data.
- Computer equipment or media that are to be sold or scrapped will have had all personal data destroyed, by re-formatting or over-writing.

If personal data needs to be retained for record keeping, it will be kept in accordance with the Minimum Retention Periods for Records Containing Personal Data:

Type of Record	Minimum Retention Period	Reason for Length of Period
Personnel files including training records, notes of disciplinary and grievance hearings, and appraisal forms.	6 years from the end of employment Certain personal data may be held in perpetuity	References and potential litigation Selected data will form part of the GCM archive
Letters of reference	6 years from the end of employment, by the author of the reference letter	References and potential litigation
Application forms/interview notes	At least 6 months from the date of the interviews	Time limits on litigation
Facts relating to redundancies	6 years from the date of redundancy	Time limits on litigation
Income Tax and NI Returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records related	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	As above	Statutory Maternity Pay Regulations (General) 1986
Statutory Sick Pay records and calculations	As above	Statutory Suck Pay Regulations (General) 1982
Wages and salary records	7 years	Taxes Management Act 1970
Finance Records	7 years	
Trustee minutes and reports	Lifetime of the charity	
Safeguarding Reports	Not to be destroyed	
DBS Records	6 months after an employee/volunteer has left	https://www.gov.uk/government/publications/handling-of-dbs-certificate-information/handling-of-dbs-certificate-information
Accident books, and records and reports of accidents	3 years after the date of the last entry	Social Security Claims and Benefits Regulations1979 , RIDDOR 1985 Health and Safety at Work Regulations

Health Records	During employment	Medical records kept by reason of the COSHH Regulations 1999
Health Records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical records kept by reason of the COSHH Regulations 1999	40 Years	COSHH Regulations 1999
Ionising Radiation Records	At least 50 years after last entry	Ionising Radiations Regulations 1985

Should an individual request to restrict the use of their personal data, the identity of the individual will be verified using the personal data currently stored and the request will be responded to without delay and within a month of receipt. The request will be managed by the Office Manager and passed on for processing to the necessary people using the data processing flowchart. Deletion of personal data is not always necessary and will depend of the restriction request.

Should an individual object to the use of their personal data, the identity of the individual will be verified using the personal data currently stored and the request will be responded to without delay and within a month of receipt. The request will be managed by the Office Manager and passed on for processing to the necessary people using the data processing flowchart. Deletion of personal data is not always necessary and will depend of the restriction request.

Should an individual request to move, copy, or transfer their personal data form Information Technology (IT) environment to another, the identity of the individual will be verified using the personal data currently stored and the request will be responded to without delay and within a month of receipt. The request will be managed by the Office Manager and passed on for processing to the necessary people using the data processing flowchart. Every effort will be made to ensure that the transfer is made securely and to an IT environment that abides by GDPR principles.

Should information be transferred out of the European Economic Area, an adequate level of protection will ensure that the data is being processed in accordance with GDPR principles.

Information risks are managed by the Data Controller and Data Protection Impact Assessments are carried out when using new technologies, or the processing is likely to result in a high risk to the rights and freedoms of individuals.

GCM is registered with the Information Commissioners Office (ICO).

5. Processing of Sensitive Personal Data

Sensitive personal data includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation. This data will be only obtained when necessary and when consent has been given by the individual. A separate consent form will be given for each category of sensitive personal data being obtained.

Criminal conviction and offence data will only be processed under the authority and control of the Disclosure and Barring Service.

6. Subject Access Requests

A subject access request is often used by individuals who want to see a copy of the information an organisation holds about them.

Requests from individuals to access their personal data should be made in writing. The identity of the individual will be verified using the personal data currently stored and the request will be responded to without delay and within a month of receipt. The individual must be told whether any personal data is being processed; given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; given a copy of the information comprising the data, and given details of the source of the data (where this is available).

A fee of £10 will be charged to the individual.

7. Process for Reporting Breaches in Data Protection

All staff, volunteers, and Trustees have an obligation to report data protection breaches or contact the Data Protection
Officer if they have concerns of such a 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. It also means that a breach is more than just about losing personal data.

In the event of discovering a breach, staff, volunteers, and Trustees should report the breach to the Data Protection Officer. The breach will then be investigated further and appropriate steps will be taken to fix the issue in a timely manner. The likelihood and severity of the breach resulting risk to people's rights and freedoms will be assessed. If it is likely that there will be a risk then the Information Commissioners Office will be notified; if it is unlikely then the breach will be dealt with internally. All breaches will be documented.

8. Staff Training

Staff with specific duties around information security and database management will be provided with specialist training on the subject of General Data Protection Regulation (GDPR). All other staff and volunteers involved in the processing of personal data will be provided with in house training on the subject of Data Processing under GDPR. Staff and volunteers will be trained annually, and updated, as necessary, with any changes that effect the way they process data.

Compliance with the Data Protection Policy is monitored. Measures are tested that are detailed in the policy by the Data Protection Officer with chosen members of staff to ensure that the policy is understood and is being implemented across GCM. The compliance is done annually and the results are reported to the Trustees.

9. Privacy Notices

A privacy notice is published on the GCM website and within any forms or letters that are sent to individuals. Our privacy notice is amended depending on which category of data we are processing and include the following:

- Who we are;
- What we are going to do with the information; and
- Who the information will be shared with.

10. Consequences of Failing to Comply with the Policy

Failing to comply with this policy can result in a disciplinary hearing and, in some cases, dismissal. The outcome will depend on the seriousness of the non-compliance and will be decided by the GCM Manager and Trustees, after consultation with the Data Protection Officer.

Personal information must not be disclosed either orally or in writing or via social media or by any other means, manual or electronic, accidentally or otherwise, to any unauthorised third party. Unauthorised disclosure will be a disciplinary matter, and may be considered as gross misconduct.

Every effort will be made to ensure that decision makers adhere to data protection legislation and promote a positive culture of data protection compliance across the organization.