Data Protection Policy

Status	Approved
Trustee Board Approval	13th December 2021
Review date	May 2024
Document Location	S:\Common\Data Protection
This policy is available from www.GCUstudents.co.uk/privacy-policy.	

1. Introduction

Glasgow Caledonian University (GCU) Students' Association ("Association") is a charitable organisation whose registered address is 70 Cowcaddens Road, Glasgow, G4 0BA. The Association is a registered Scottish charity, number SC022887 and is registered with the Information Commissioner's Office, with Registration Number Z5904134.

The Association is committed to ensuring the secure and safe management of data held by the Association in relation to members (including volunteers), employees and other individuals. The Chief Executive is responsible for data protection compliance within the Association. All Association employees and volunteers have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

The Association needs to gather and use certain information about individuals. These can include members, employees and other individuals that the Association has a relationship with. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the UK GDPR).

This Policy sets out the Association's duties in processing that data, and the purpose of this Policy is to set out the procedures for the management of such data.

2. Legislation

It is a legal requirement that the Association process data correctly; the Association must collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data is:

(1) the United Kingdom General Data Protection Regulation and the Data Protection Act 2018 ("the UK GDPR");

(2) Data Protection, Privacy and Electronic Communications (Amendment etc.)(EU Exit) Regulations 2019 (SI419), The Data Protection, Privacy and Electronic Communications (Amendment etc.)(EU Exit) Regulations 2020 (SI1586), Schedule 3 of the European Union (Withdrawal Agreement) Act 2020 and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK.

3. Data

3.1 The Association holds a variety of Data relating to individuals, including members and employees (also referred to as data subjects) which is known as Personal Data. The Personal Data held and processed by the Association is detailed within the Association's Privacy Notices.

3.1.1 "Personal Data" is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by the Association.

3.1.2 The Association also holds Personal data that is sensitive in nature (i.e. relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, trade union membership, relates to health or sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data".

4. Data Protection Principles

4.1 The Association will comply with the following data protection principles when processing personal information:

4.1.1 Process personal information lawfully, fairly and in a transparent manner;

4.1.2 Collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.1.3 Process the personal information that is adequate, relevant and necessary for the relevant purposes;

4.1.4 Keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;

4.1.5 Keep personal information in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed; and

4.1.6 Take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5. Processing of Personal Data

5.1 The Association is permitted to process Personal Data on behalf of data subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject;
- Processing is necessary for the performance of a contract between the Association and the data subject or for entering into a contract with the data subject;
- Processing is necessary for the Association's compliance with a legal obligation;
- Processing is necessary to protect the vital interests of the data subject or another person; or
- Processing is necessary for the purposes of legitimate interests.

5.2 **Members Privacy Notice**

5.2.1 The Association has produced a Members Privacy Notice which it is required to provide to all members whose Personal data is held by the Association. The Members Privacy Notice is provided when members register an account on the Association website, at the bottom of every email sent and is available from www.GCUstudents.co.uk/privacy-policy.

5.2.2 The Members Privacy Notice sets out the Personal Data processed by the Association and the basis for that Processing. It will also outline, where applicable, Special Category Data, which is held and processed by the Association.

5.3 **Employee Privacy Notice**

5.3.1 The Association has produced an Employee Privacy Notice which outlines the Employee personal data and, where applicable, Special Category Data or criminal offence information, that is held and processed by the Association. The Employee Privacy Notice is provided to employees at job application stage, is available from www.GCUstudents.co.uk/privacy-policy and is available on the Shared Drive in the Data Protection Folder.

5.3.2 Employees should also refer to other relevant policies in relation to internet, email and communications, monitoring, social media, information security, data retention and bring your own device (BYOD) which contain further information regarding the protection of personal information in those contexts.

5.3.3 A copy of any employee's Personal Data held by the Association is available upon written request by that employee.

5.4 **Consent**

Consent as a ground of processing will require to be used from time to time by the Association when processing Personal Data. It should be used by the Association where no other alternative ground for processing is available. In the event that the Association requires to obtain consent to process a data subject's Personal Data, the Association shall keep a record of the consent obtained from the individual. Any consent to be obtained by the Association must be for a specific and defined purpose (i.e. general consent cannot be sought).

5.5 **Legitimate Interests**

When determining whether legitimate interests is the most appropriate basis for lawful processing data, the Association will:

5.5.1 Conduct a legitimate interests' assessment (LIA) and keep a record of it, to ensure that the Association can justify its decision; (a LIA is a process whereby you establish why the Association have selected Legitimate Interest as the basis for processing your information; the Information Commissioner's Office sets out three elements to this process 1) identify a legitimate interest; 2) show that the processing is necessary to achieve it; and 3) balance it against the individual's interests, rights and freedoms)

5.5.2 Keep the LIA under review, and repeat it if circumstances change; and

5.5.3 Include information about legitimate interests in the Association relevant privacy notice(s).

5.6 **Processing of Special Category Data or Sensitive Personal Data**

5.6.1 Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'. In the event that the Association processes Special Category Personal Data or Sensitive Personal Data, the Association must have a lawful basis and do so in accordance with one of the following grounds of processing:

(a) the data subject has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Association or the data subject;

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) processing relates to personal data which are manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) the processing is necessary for reasons of substantial public interest.

5.6.2 Employees and volunteers must seek authorisation from the Chief

Executive before processing sensitive personal data.

5.7 **Criminal Records Information**

Where the Association requires to process criminal records information, it will be processed in accordance with the data protection principles.

5.8 **Concerns**

You should contact the Chief Executive if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

5.8.1 Processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in section 5.6 being met;

5.8.2 Any data breach as set out in section 8 below;

5.8.3 Access to personal information without the proper authorisation;

5.8.4 Personal information not kept or deleted securely;

5.8.5 Transfer of personal information without appropriate security measures being in place;

5.8.6 any other breach of this policy or of any of the data protection principles set out in section 4.

6. Data Sharing

6.2 The Association shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with the Association's relevant policies and procedures. In order that the Association can monitor compliance by these third parties with Data Protection laws, the Association will require the third party organisations to enter in to an Agreement with the Association governing the processing of data, security measures to be implemented and responsibility for breaches.

6.3 The Chief Executive will approve any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement being altered.

6.4 Data Sharing

6.4.1 Personal data is from time to time shared amongst the Association and third parties who require to process personal data that the Association process as well. Both the Association and the third party will be processing that data in their individual capacities as data controllers.

6.4.2 Where the Association shares in the processing of personal data with a third party organisation, it shall require the third party organisation to enter in to a Data Sharing Agreement with the Association.

6.5 Data Processors

A data processor is a third party entity that processes personal data on behalf of the Association.

6.5.1 A data processor must comply with Data Protection laws. The Association's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify the Association if a data breach is suffered.

6.5.2 If a data processor wishes to sub-contact their processing, prior written consent of the Association must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

6.5.3 Where the Association contracts with a third party to process personal data held by the Association, it shall require the third party to enter in to a processing agreement with the Association.

7. Data Storage and Security

All Personal Data held by the Association must be stored securely, whether electronically or in paper format.

7.1 Paper Storage

If Personal Data is stored on paper it should be kept in a secure place where unauthorised individuals cannot access it. Employees and volunteers should make sure that no Personal Data is left where unauthorised individuals can access it. When the Personal Data is no longer required it must be securely disposed of by the employee or volunteer so as to ensure its destruction.

7.2 Electronic Storage

Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data (or the device storing the data) should be password protected or encrypted when being sent internally or externally to the Association's data processors or those with whom the Association has entered in to a Data Sharing Agreement.

7.3 The GCU Data Protection website provides guidance on Information Security. More information: www.gcu.ac.uk/dataprotection.

8. Breaches

8.1 A data breach can occur at any point when handling Personal Data and the Association has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported to the Information Commissioners Office (ICO).

8.2 A data breach may take many different forms, for example:

8.2.1 loss or theft of data or equipment on which personal information is stored;

8.2.2 unauthorised access to or use of personal information either by an employee, volunteer or third party;

8.2.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

8.2.4 human error, such as accidental deletion or alteration of data;

8.2.5 unforeseen circumstances, such as a fire or flood;

8.2.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

8.2.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

8.3 **Internal Reporting**

The Association takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred the Chief Executive must be notified of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- The Association must seek to contain the breach by whatever means available;
- The Chief Executive in consultation with professional and/or legal advisors, must consider whether the breach is one which requires to be reported to the ICO and data subjects affected;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

8.4 **Reporting to the ICO**

The Chief Executive will require to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the Information Commissioner's Office ("ICO") within 72 hours of the breach occurring. The Chief Executive must also consider whether it is appropriate to notify those data subjects affected by the breach.

9. Data Subject Rights

9.1 Certain rights are provided to data subjects under the UK GDPR. Data Subjects are entitled to view the personal data held about them by the Association, whether in written or electronic form.

9.2 Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to the Association's processing of their data. These rights are notified within the Association's Privacy Notice.

9.3 **Subject Access Requests**

Data Subjects are permitted to view their data held by the Association upon making a request to do so (a Subject Access Request). Upon receipt of a request by a data subject, the Association must respond to the Subject Access Request within 28 days of the date of receipt of the request. The Association:

9.3.1 must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law.

9.3.2 where the personal data comprises data relating to other data subjects, must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the Subject Access Request, or

9.3.3 where the Association does not hold the personal data sought by the data subject, must confirm that it does not hold any personal data sought to the data subject as soon as practicably possible, and in any event, not later than 28 days from the date on which the request was made.

9.4 **The Right to be Forgotten**

9.4.1 A data subject can exercise their right to be forgotten by submitting a request in writing, or verbally, to the Association seeking that the Association erase the data subject's Personal Data in its entirety.

9.4.2 Each request received by the Association will require to be considered on its own merits and professional and/or legal advice will require to be obtained in relation to such requests from time to time. The Chief Executive will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.4 and will respond in writing to the request.

9.5 **The Right to Restrict or Object to Processing**

9.5.1 A data subject may request that the Association restrict its processing of the data subject's Personal Data, or object to the processing of that data.

9.5.2 In the event that any direct marketing is undertaken from time to time by the Association, a data subject has an absolute right to object to processing of this nature by the Association, and if the Association

receives a written or verbal request to cease processing for this purpose, then it must do so immediately.

9.5.3 Each request received by the Association will require to be considered on its own merits and professional and/or legal advice will require to be obtained in relation to such requests from time to time. The Chief Executive will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.5 and will respond in writing to the request.

10. Privacy Impact Assessments ("PIAs")

10.1 These are a means of assisting the Association in identifying and reducing the risks that operations have on personal privacy of data subjects.

10.2 The Association shall:

10.2.1 Carry out a PIA before undertaking a project or processing activity which poses a "high risk" to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data; and

10.2.2 In carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data

10.3 The Association will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The Chief Executive will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the Chief Executive within five (5) working days.

11. Archiving, Retention and Destruction of Data

The Association cannot store and retain Personal Data indefinitely. It must ensure that Personal data is only retained for the period necessary. The Association shall ensure that all Personal data is archived and destroyed in accordance with the periods specified within the Retention Schedule.

12. Review and Monitoring

The Association will review and update this Policy in accordance with data protection obligations. This Policy does not form part of an employee's contract of employment and the Association may amend, update or supplement it from time to time. The Association will circulate any new or modified policy to

members and employees before it is adopted. The latest version of this Policy will be available on www.GCUstudents.co.uk/privacy-policy.