



Data Protection Policy

Status	APPROVED
Trustee Board Approval	5 th October 2026
Review date	May 2028
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 Commission, 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).

The Association manages a significant amount of data, from a variety of sources but receives most data about its members from Glasgow Caledonian University.

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) the Data (Use and Access) Act 2025 ("DUAA");
- (3) the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR");
- (4) any legislation that, in respect of the United Kingdom, replaces, or enacts into the United Kingdom domestic law, the UK GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003 or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union.

3. Data

- 3.1 The Association holds a variety of Data relating to living individuals, including members and employees (also referred to as data subjects). Data which can identify data subjects and relates to them 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 and which relates to the individual.
 - 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". The Secretary of State may designate further categories of Special Category Personal Data and if this occurs the Association shall treat any such designated data accordingly.

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 purpose for which it is processed;
 - 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;
- Processing is necessary for the purposes of the legitimate interests pursued by the Association or by a third party; or
- Processing is necessary for the purposes of a recognised legitimate interest.

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 subject to certain exemptions.

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). The consent provided by a data subject must be freely given and they are free to withhold their consent or withdraw it at any future time.

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 Commission 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 Personal Data or Criminal Offence 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 Criminal Offence Data, the Association must rely on an additional ground for processing in accordance with one of the special category grounds. These included, but are not restricted to, the following:

- (a) the data subject has given explicit consent to the processing of this data for a specified purpose;
- (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 or, if the data subject is incapable of giving consent, the vital interests of another person;
- (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 whenever courts are acting in their judicial capacity; and
- (f) the processing is necessary for reasons of substantial public interest under law.

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

- 6.1 The Association is responsible for the processing of personal data by third parties or individuals working on its behalf.
- 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 into 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 The Association has a Data Sharing Agreement with Glasgow Caledonian University.

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.
- 6.5.4 The Association will take a data protection by design approach at the outset of any processing of personal data involving AI. This can be demonstrated by using a Data Protection Impact Assessment (DPIA) to identify, assess and appropriately address any risks arising from a specific use of Generative AI.
- 6.5.5 Any agreements concluded concerning personal data that is transferred outside of the UK to a country not covered by a UK "Adequacy Decision" must be accompanied by an "International Data Transfer Agreement" ("IDTA") or other approved transfer mechanism. The Association shall complete a Data Protection Test to reasonably and proportionately document and review whether the data protection standards in the destination country are not materially lower than the standard of protection provided under UK data protection laws.

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, as outlined in our Retention Schedule, it must be securely disposed of by the employee or volunteer so as to ensure its secure 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 Commission.

- 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 Information Commission and data subjects affected;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements, Data Processing Agreement or equivalent contractual terms.

8.4 Reporting to the Information Commission and to Data Subjects

The Chief Executive will be required 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 Commission (“IC”) within 72 hours of the breach occurring or the Association becoming aware of the breach. The Chief Executive must also consider whether it is appropriate to notify those data subjects affected by the breach.

Where a breach poses a high risk to the rights and freedoms of the Data Subjects impacted by the breach, the Association must, in addition to notifying the Information Commission, promptly notify the Data Subjects in question.

9. Data Subject Rights

9.1 Certain rights are provided to data subjects under data protection laws:

- 9.1.1 a right to be informed about the collection and use of their personal data (typically fulfilled by providing individuals with a Fair Processing Notice) (the “right to be informed”);
- 9.1.2 a right to access and receive a copy of their personal data, plus other supplementary information (the “right of access”);
- 9.1.3 a right to have inaccurate personal data rectified and incomplete personal data completed (the “right to rectification”);
- 9.1.4 a right to have personal data erased (the “right to erasure”);
- 9.1.5 the right to request the restriction or suppression of personal data (the “right to restrict”);
- 9.1.6 the right to obtain and reuse certain personal data across different providers (the “right to data portability”);
- 9.1.7 the right, in certain circumstances, to object to the processing of their personal data (the “right to object”);
- 9.1.8 the right to make a complaint about how their personal data has been processed (the “right to complain”); and

- 9.1.9 rights to protect individuals against automated decision making or profiling (“rights related to automated decision making”).
- 9.2 These rights are notified to the Association’s members (including volunteers), employees and other individuals in the Association’s Privacy Notices. Such rights are subject to qualification and are not absolute.
- 9.3 Each request received by the Association will require to be considered on its own merits and 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 and will respond in writing to the request.
- 9.4 **Right of Access: 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) subject to certain exemptions. 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 (unless the Association is entitled under the relevant legislation to increase the timescale). The Association:
- 9.4.1 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.
- 9.4.2 where the personal data comprises data relating to other data subjects, the Association shall only release the data where: the Association has obtained consent from those data subjects OR the Association determines it is reasonable to disclose said data without consent, or
- 9.4.3 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.
- 9.5 **The Right to Complain**
- 9.5.1 A data subject may complain to the Association if they consider their personal data has been processed by the Association in contravention of data protection law.
- 9.5.2 Any such complaint will be handled in accordance with the Association’s Complaints Procedure. Complaints received in relation to the Association’s handling of personal data will be acknowledged within 30 days in line with the Data (Use and Access) Act 2025.
- 9.5.3 Individuals will be made aware of their right to escalate to the Information Commission if they are dissatisfied with the Association’s response.

10. Data Protection Impact Assessments (“DPIAs”)

- 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 DPIA before undertaking a project or processing activity which poses a “high risk” to an individual. 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 DPIA, 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 Information Commission in the event that a DPIA identifies a high level of risk which cannot be reduced or mitigated. The Chief Executive will be responsible for such reporting, and where a high level of risk is identified by those carrying out the DPIA 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. CCTV

CCTV is used for the purposes of the prevention of crime and to protect public safety and the security of the University community. CCTV is managed by Glasgow Caledonian University. The University has a separate CCTV policy in place.

13. 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.