Glasgow Kelvin College

Data Protection Policy

Document Control Information	
Reviewed by the Senior Management Team:	**March 2023**
Date of Next Review:	**March 2026**
Approved by the Board of Management:	**March 2023**

The Board of Management (or any person/group with delegated authority from the Board) reserves the right to amend this document at any time should the need arise following consultation with employee representatives. This Policy has been subject to an Equality Impact Assessment, which is published on our website: https://www.glasgowkelvin.ac.uk/equality-diversity/

1. Introduction

The purpose of this document is to set out the College's data protection policy. This policy document provides the overarching framework within which the College processes and manages personal data and manages personal data to deliver learning, teaching and other operational functions. This policy ensure that we treat personal information lawfully and in a way which complies with data protection law.

This policy applies to all:

- college users including past, present and prospective staff, students, contractors and Board of Management members[1], students, contractors, partners and third parties acting on our behalf;
- all personal and special category 'sensitive' (for example health) data collected, processed, created, stored and disclosed by the College across all formats (including but not limited to physical paper documents, photographs, CD's/DVD's, electronically (for example websites and emails) or other methods of sharing documents online including SharePoint, cloud storage services and verbally in conversation or by telephone (where recorded) of any age;
- all locations from which College personal data is accessed including home or remote working use;
- transfer of data overseas;
- direct marketing; and
- security, including CCTV.

All college users must comply with this policy and the processes and procedures which support it. College managers who have responsibility for data and electronic systems must ensure that their team procedures and processes comply with this policy. These managers are part of the College's Privacy Network.

2. Data Protection Policy Aims

Glasgow Kelvin College must collect and use certain types of information about its users to achieve its aims and deliver its mission.

We process personal information so we can perform our duties including:

- providing education, support and general advice services for our students and facilities to our clients
- promoting the college and our services
- publishing the college news articles
- maintaining our own accounts
- supporting and managing our staff.

We also process CCTV to maintain the safety and security of college users, premises and assets and for preventing, detecting and investigating criminal or disciplinary offences.

All personal information is processed, stored, shared and destroyed in a manner which is fully compliant with the data protection law, regardless of the format or media on which it is collected, processed and stored.

3. The College Data Protection Policy covers the following key aspects:

- The College will ensure that it complies with the Data Protection Principles;
- The College will ensure that it has processes in place to enable data subjects to exercise their rights in respect of their data;
- The College will put in place specific measures to protect any special category data it holds;
- The College will ensure accountability for the processing of personal data.

The College, as a data controller, is accountable for the data it collects, processes, stores, shares and destroys and will only do this where necessary. Particular care will be taken in respect of special category data, this is defined as data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, Trade Union membership or the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health and data concerning a natural person's sex life or sexual orientation. Stricter security and access control measures shall be in operation in respect of all such data sets.

4. The Data Protection Principles

The College will seek to ensure that all of its systems, processes and procedures comply with the Data Protection Principles, specifically data will be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;

2. 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;

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. 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;

5. kept in a form 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

6. 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.

5. Rights of the Data Subject

The College is also committed to ensuring that the rights of data subjects are fully respected and that its systems and processes will enable data subjects to exercise their rights which are embedded in law. Data subjects (individuals whose data is being processed) have the following rights in respect of personal data the College processes about them:

Data subjects (individuals) have the following rights in respect of the data the College has which relates to them:

1. the right to be informed;
2. the right of access;
3. the right to rectification;
4. the right to erasure;
5. the right to restrict processing;
6. the right to data portability;
7. the right to object; and
8. the right not to be subject to automated decision making or profiling.

These rights, however, are not absolute. The College policy is that it will seek to ensure that it has in place systems which enable data subjects to exercise their rights and can appeal and complain about decisions made by the College in this regard. The College will also ensure that there are appropriate measures in place for children (under 13 years of age) and other individuals who are not able to provide consent to data collection and processing themselves.

6. Control Measures

Glasgow Kelvin College will, through appropriate management structures, systems and processes;

1. observe fully conditions regarding the fair collection and use of information;

2. meet its legal obligations to specify the purpose for which information is used;

3. collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;

4. ensure the quality of information used;

5. apply strict checks to determine the length of time information is held;

6. ensure that the rights of people about whom information is held are able to be fully exercised under the Act;

7. take appropriate technical action and organisation security measures to safeguard personal information;

8. ensure that personal information is not transferred without permission and appropriate safeguards; and

9. ensure staff are trained in data protection.

7. Accountability

The College requires all staff to exercise responsibility, integrity and care in handling and processing personal data. In particular, staff must treat all personal data confidentially and must not share or disclose personal data to external individuals or organisations unless it is permitted by the data subject, is permitted by college processes and procedures or a member of the Senior Management Team.

The College will ensure that:

- all members of the Senior Management Team are trained in data protection;
- there are named individuals with specific responsibility for data protection within the college (nominated persons: Vice Principal Operations and Director of Estates and Corporate Services);
- there is a designated Data Protection Officer; and
- the CCTV system in use for security and crime prevention purposes satisfies the Information Commissioners Office requirements.

Those who supervise data processing (members of the operational management team and other College managers), have special obligations to ensure that they have established procedures within their specific areas of responsibility which are fully implemented, and that staff are aware of their responsibilities which are summarised below:

- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice, complying with College policies/procedures and the data protection legislation;
- everyone managing and handling personal information is appropriately trained to do so and appropriately supervised;
- paper files are kept appropriately secure and ICT security protocols and procedures are followed fully by all staff;
- personal data is not shared outside the College without appropriate consent and only where it is compliant with the Privacy Notice in place[2]

- systems will be configured in a way which enables them to enable individuals to exercise their rights (as stated above);
- queries about handling personal information are promptly and courteously dealt with;
- a regular review is made of the way personal information is managed;
- confidential paper records are securely disposed of within the terms of the College's data retention schedule;
- redundant ICT equipment is recycled using the services of a contractor who sanitises all hard drives;
- College mobile devices can be remotely wiped;
- Staff laptops are encrypted;
- performance with handling personal information is regularly assessed and evaluated; and
- methods of handling personal information are regularly assessed and evaluated.

8. Further information

A diagram detailing the way in which data protection and information governance is managed by the College is detailed in Appendix 1 - Information Governance – Privacy Network.

All staff are encouraged to contact their line manager, the Director of Estates and Corporate Services or the Data Protection Officer in the event that they require guidance on the content of this policy, its application or the application of the procedures which support it.

The processes and procedures which support this policy are as follows:

- Data Breach Notification
- Data Retention Schedule
- Subject Access Request Process
- Individual Rights under GDPR

[1] It should be noted that Board members are also charity trustees and any reference to Board members in College policy documents also refers to that role.

[2] Privacy Notices are available for review on the College website; any material changes to these notices will be communicated to data subjects accordingly.

Appendix 1 – Information Governance – Privacy Network