



Data Protection — GDPR Policy

Homerton College is fully committed to comply with the General Data Protection Regulation (GDPR). After 25 May 2018, the GDPR applies to all Colleges that process data relating to their employees, as well as to others including customers, contractors and clients. It sets out principles which should be followed by those who process data; it gives new and extended rights to those whose data is being processed.

To this end, Homerton College endorses fully and adheres to the six principles of data protection, as set out in the Article 5 of the GDPR.

Seven key principles

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.

1. (Lawfulness, fairness and transparency: - data is processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Purpose limitation – data is 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. Data minimisation - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accuracy – data is 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. Storage limitation – data is 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.
6. Integrity and confidentiality – data is 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.
7. Accountability - the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1.

These principles must be followed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the College will:

- observe fully the conditions regarding the fair collection and use of information including the giving of consent;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- ensure that the information is held for no longer than is necessary;
- ensure that the rights of people about whom information is held can be fully exercised under the GDPR (ie the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as incorrect);

- take appropriate technical and Collegial security measures to safeguard personal information;
- publicise and abide by individuals' right to appeal or complain to the supervisory authority (the Information Commissioner's Office (ICO)) in the event that agreement cannot be reached in a dispute regarding data protection; and
- ensure that personal information is not transferred abroad without suitable safeguards.

Scope and Status of this Policy

All academic and non-academic staff.

The Policy does not form part of the formal contract of employment for employees but it is a condition of employment that employees will abide by the rules and policies of the College. Any failure to follow the Data Protection Policy may lead, therefore, to disciplinary proceedings.

Designated Data Protection Officer (DPO) and College Data Protection Lead (CDPL)

At Homerton, the role of DPO is taken by the Office of Intercollegiate Services (OIS). As OIS is a separate entity from the College, the responsibility for acting as the first line of contact for data subjects has been delegated to a senior member of College staff. The Tutorial Office Manager and the Tutorial Office Coordinator share the role of College Data Protection Lead (CDPL) and work closely with the DPO to investigate and report any (potential) breaches. Any (potential) breaches should be discussed with the CDPLs in the first instance. The CDPLs can be contacted via the dataprotection@homerton.cam.ac.uk email. We only have 72 hours to report a breach from the time we become aware of it.

Employee Responsibilities

All employees are responsible for:

- checking that any information that they provide to the College in connection with their employment is accurate and up to date
- informing the College of any changes to information that they have provided, e.g. changes of address, either at the time of appointment or subsequently. The College cannot be held responsible for any errors unless the employee has informed it of such changes.

Data Security

All employees are responsible for ensuring that:

- any personal data that they hold is kept securely
- personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Employees should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be coded, encrypted or password protected both on a local hard drive 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 filing cabinet, drawer, or safe.

- Advise the CDPL of any data breaches as soon as possible. See Appendix A for the Data Breach Reporting process.

Personal data breaches will be required to be communicated to the ICO by the DPO 'without undue delay' and in any event within 72 hours of the breach being identified unless the breach is unlikely to result in a risk to the rights and freedoms of the data subjects. The breach report will need to include:

- The nature of the breach, including an approximate number of data subjects involved and the categories of personal data affected;
- The likely consequences of the breach; and
- The measures taken or proposed to address the breach and measures being taken to mitigate the stated consequence

The College will also communicate to all affected data subjects without undue delay (unless the breach is unlikely to result in a high risk to the rights and freedoms of the data subjects). There are circumstances where such communications is not required:

- Where general measures (technological and organisational) have been adopted to render the personal data as unintelligible to any person not authorized to access it. Eg through encryption or robust password protections.
- Where subsequent actions have removed the risk of the rights or freedoms of data subjects beyond likelihood
- Where such communication would be one of disproportionate effort providing that the College makes an appropriate public statement instead so that data subjects are informed in an equally effective manner.

Disaster Recovery

1. Homerton College backs up data every day and has multiple copies (at least one set for each day of the week and additional weekly ones in order to have at least a month's worth of data at any one time). Records of these are kept.
2. Backups are kept on site are in special heat-proof safes: fire-proofing alone is inadequate.
3. Backups are verified regularly by the software and system supplier.
4. Firewalls and virus checkers are kept up to date and running, and users are trained in virus avoidance and detection.
5. Computers are protected from physical harm, theft or damage, and from electrical surges using protective plugs.
6. The College plans for how to deal with loss of electricity, external data links, server failure, and network problems. It uses paper forms where necessary for temporary record keeping.

Subject Consent

The GDPR sets a high standard for consent and requires a positive opt-in. Neither pre-ticked boxes nor any other method of default consent are allowed. As required by the GDPR, the College takes a "granular" approach ie it asks for separate consent for separate items and will not use vague or blanket requests for consent. As well as keeping evidence of any consent, the College ensures that people can easily withdraw consent (and tells them how this can be done).

It should be noted, however, that consent is only one of the lawful bases on which data processing depends. In brief, the others include the following.

- **Contract:** if processing someone's personal data is necessary to fulfil the College's contractual obligations to them (eg to provide a quote).
- **Legal obligation:** if processing personal data is necessary to comply with a common law or statutory obligation.
- **Vital interests:** not one that will occur often as it refers to processing personal data to protect someone's life (and even then, it cannot be relied on with regard to health data or other special category data if the individual is capable of giving consent).
- **Legitimate interests:** the most flexible lawful basis for processing and one which applies when data is used in ways people would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

Note that the GDPR provides for special protection for children's personal data and the College will comply with the requirement to obtain parental or guardian consent for any data processing activity involving anyone under the age of 16.

Data Subject Access Request

Under data protection legislation an individual (data subject) has the right, subject to certain exemptions, to access the personal information that an organisation holds about them.

Accessing personal data in this way is known as making a data subject access request.

If a data subject would like a copy of the information held on them, they should write to the College Data Protection Lead at Homerton College, Cambridge CB2 8PH, or dataprotection@homerton.cam.ac.uk. They may apply to access their data in writing in any way they choose. The Data Subject Access Request Form (see Appendix B) can be used for this purpose.

Before we can act on a request, we must:

- be sure of the data subject's identity
- be supplied with information from the data subject in order to locate the information they seek

The data subject is entitled to:

- be informed whether their personal data is being processed by Homerton College
- have the information constituting the personal data communicated to them in a permanent form (usually, this means paper copies)
- be given a summary of the sources, recipients and purposes of the processing

On receipt of the completed request, verification of their identity, and sufficient details to enable us to locate the information, the requested information will be provided within 30 calendar days. The information will be supplied subject to any applicable exemptions. The data will be provided as of the date of receipt of the request. If there is any reason for delay, that will be communicated within the 30 days' time period. A request which is manifestly unfounded or excessive may be refused. The person concerned will then be informed of their right to contest this decision with the supervisory authority (the ICO).

If a data subject believes that any information held on them is incorrect or incomplete, or if they have any reason to believe that the Homerton College has not dealt correctly with the request, please contact data.protection@admin.cam.ac.uk. If they are still not satisfied, they should contact the [Information Commissioner's Office](https://ico.org.uk/concerns/) at <https://ico.org.uk/concerns/>

Subject access requests are different to requests submitted under FOI legislation, which relate to information about the organisation itself.

Right to be forgotten

Homerton College recognises the right to erasure, also known as the right to be forgotten, laid down in the GDPR. Individuals should contact the College Data Protection Lead with requests for the deletion or removal of personal data. These will be acted on provided there is no compelling reason for continued processing and that the exemptions set out in the GDPR do not apply. These exemptions include where the personal data is processed for the exercise or defense of legal claims and to comply with a legal obligation for the performance of a public interest task or exercise of official authority.

Policy change history		
Date	Summary of Changes	Date of next review
April 2018	New policy in line with GDPR legislation	
November 2021	Update to reflect additional principle, changes to DPO and CDPL, and inclusion of Appendix A and B in the policy	November 2023
March 2025	Update changes to CDPL	March 2027



Appendix A – Data Breach Reporting Process

1. When somebody becomes aware of a data breach, it needs to be reported **within 72 hours**.
2. Should an employee make you aware of a data breach, you have to immediately ask them to get in touch with the College Data Protection Lead on dataprotection@homerton.cam.ac.uk who will ask them to complete Section A of the Personal Data Incident Report (PDIR). The person who reported the breach will also be asked to forward any other relevant information eg email etc.
3. Where it is possible, put immediate steps in place to limit damage, eg somebody was forwarded an email by mistake, the employee needs to ask the unintended recipient(s) as well as other recipient to delete the message to avoid anybody accidentally responding to an email again. They need to confirm that this has been done and all messages must be kept.
4. The College Data Protection Lead will review the PDIR, complete Section B and forward the completed form to the Data Protection Officer together with any additional information which will help them to review the breach. The OIS will then complete Section C and advise us on next steps, i.e whether it is necessary to inform the ICO.
5. The DPO would also make suggestions to avoid a similar breach going forward and it is important to share that and put any steps in place as suggested.
6. Where it is necessary to inform the ICO, the DPO will provide guidelines.



Appendix B – Data Subject Access Request Form

The following information is needed to help us give a quick and accurate response to your enquiry. Please complete the information below and return the form by post or email to the College Data Protection Lead at dataprotection@homerton.cam.ac.uk .

Part A. Your request

Title:	
Surname:	
Forename(s):	
Address:	
Telephone number:	
Email address:	
Other name by which you have been known, if applicable:	
Relationship to Homerton College:	

Please provide a description of your request, and any further information which will enable us to locate your personal data (continue overleaf if necessary).

Part B. Proof of identity

The GDPR requires the College to satisfy itself as to the identity of the person making the request. Please send a photocopy of one form of identification containing a photograph (e.g. University Card, Passport, Photocard Driving License) to the Data Protection Officer, email: dataprotection@homerton.cam.ac.uk. If the supply of this documentation is problematic please contact us to discuss alternative proof of identity arrangements. If the College is unable to satisfy itself as to your identity from the documentation you send us, we will contact you as soon as possible.

Part C. Declaration

I am the Data Subject named in Part A of this document, and hereby request, Homerton College provides me with copies of my personal data as described in Part A. I have provided my proof of identity.

Signature:

Date: