



Information Management Policy

Version 9.1

City College of London



Document Version Control			
Document Version	Date	Policy Author(s)	Review Date
Version 1.0	11/02/21	Mikail Huda	11/02/22



Table of Contents

Overview	5Legal Framework	5Data Requirements	5Sensitive Personal Data
	5Statutory Purposes	6Data Management	6Data Collection
	7Data Retention and Storage	7Storage of Assessment Material	7Responsibilities
	7Data Disclosure	8Disclosing information concerning members	8Protecting identities
	9Learners' Rights	10Disposal of Information	10Staff training
	10References	10Marketing Activities	10Public Information Reliability & Communication Channels
	11Completeness and accuracy procedures	12Pre-enrolment	12Post-enrolment
	12External References	13Monitoring effectiveness of publishing arrangements	
	13Representation	13External Bodies	13Copyright Laws
	13Usage of the Internet and E Mail	14Personal Use	14Prohibited Internet and Email Usage

This policy may be used in conjunction with the following policies and documents:

Policies:	Other Documents
2.1 Recruitment and Admissions Policy	Complaints Form
3.1 Staffing Policy	Job Application Form
4.1 Teaching, Learning and Assessment Policy	Learner Application Form
6.1 Equality and Welfare Policy	
8.1 Complaints and Appeals Policy	

Quality Code Reference																	
A1	A2	A3	A4	A5	A6	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	C
											X	X			X		X



Overview

The purpose of this policy is to enable City College of London to:

- Comply with the law in respect of the data it holds about individuals;
- Follow good practice;
- Protect City College of London's staff, members, service users and other individuals

We recognise that the management of data is fundamental to the effective operations of City College of London as an organisation. Some of this information is that which we wish to present, and constitutes the public image of the Academy.

Other data is of a personal and sensitive nature which necessitates arrangements to ensure confidentiality is upheld with disclosure only in those circumstances where a legal or welfare obligation is present and that the individuals in question understand these conditions.

Legal Framework

The Data Protection Act 1998 regulates the collection, storage, use and disclosure of information about individuals by organisations. Any organisation that keeps information about individuals must comply with the act. The Act applies to *personal data* - information about identifiable living individuals that is:

- Held on computer or any other automated system
- Held in a *relevant filing system* (a paper system such as client records system, or a set of files on service users that is organized alphabetically by the name of the person or some other identifier such as case number)
- Intended to go onto computer or into a relevant filing system

The Data Protection Act sets out eight enforceable principles of good practice. These principles are that the data must be:

- Fairly and lawfully processed;
- Processed for limited purposes and not in any manner incompatible with those purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept for longer than is necessary;
- Processed in accordance with individuals' rights;
- Secure

Data Requirements

City College of London needs to collect and use personal data (see paragraph below) about our service users, employees and other individuals, who are referred to in the Act as "data subjects" in order to carry out our business effectively and provide high quality services. We hold information about data subjects for service provision, administrative, personnel management and membership management purposes.

Sensitive Personal Data

The Act defines "sensitive personal data" as personal data consisting of information as to racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; membership of a trade union; physical or mental health or condition; sexual life; the commission or alleged commission of any offence or any proceedings for any offence committed or alleged to have been committed, including the disposal of such proceedings or the sentence of any court in such proceedings.



The purpose for which we hold sensitive personal data about data subjects is for use solely for equal opportunities monitoring or for the provision of specific services to individuals. This includes but is not limited to: the provision of services to members and service users, assessing suitability and fitness for work, administering sick pay and sick leave, absence control, maternity leave and pay, parental leave, paternity leave and pay, adoption leave and pay, safe environment, complying with our obligations under the Disability Discrimination Act.

Statutory Purposes

In addition to the purposes outlined above, we may collect, hold and process data including sensitive personal data if it is necessary to do so for compliance with any statutory duty with which we are required to comply. Any changes in these details (contact info, visa status etc.) must be disclosed to the Academy

Data Management

City College of London has mechanisms in place to ensure the principles of the Data Protection Act 1998 are adhered to. This section provides guidance to all staff, on their obligations in respect of accessing, holding or using personal information during the course of their employment or such as service user information and information relating to other members of staff. It applies to all employees. Those managing others should take particular notice of content, however, since they may have additional responsibilities under the Act. City College of London will ensure that:

- There is someone with specific responsibility for data protection within the organisation
- All personal information collected will be factual and objective
- All those who manage and handle personal information understand the requirements of the Act and their responsibilities under it
- All those who manage and handle personal information are appropriately trained and supervised to do so
- The methods of handling personal information are regularly audited, reviewed and evaluated

Data Collection

In order to ensure a rigorous process that provides the capacity for both audit and reflection, City College of London will ensure the collation and analysis of learner data pertaining to the following criteria:

- Initial enquiry conversion
- Acceptance and CAS issue
- Arrival and enrolments
- Retention rate (indicating drop-outs and course transfers where appropriate)
- Attendance rate
- Progress monitoring (including ILP's, tracking sheets, formative and summative assessment data)
- Completion rate
- Success rate (passes/fails)
- Exit routes (wherever possible)
- Student feedback



Analysis of the data arising from this process will be conducted per course at the end of each cohort and a report published containing the findings (per course and institutional) and any recommendations based upon any potential issues identified. From this report an action plan will be drafted and implemented.

Photographs

We will request consent before taking any photographs of individuals and will let them know how any photographs will be used.

Data Retention and Storage

All data held on individuals will be kept in two forms, one electronic (soft copy) and one paper based (hard copy). Access to the data is restricted to a limited number of staff members whose responsibility it is to oversee the appropriate maintenance and collation of such data. Information will be held for a period of five years after the individual concerned has ceased association with the Academy.

This is managed through the Customer Relationship Management (CRM) system. This is an online system that enables data for all students to be closely monitored and integrated, allowing for the effective development of our approach to student's educational and welfare provision. This system is also fully compliant with our legal data retention duties. All data held on the CRM is also reflected in our administration at the respective sites.

Storage of Assessment Material

Assessment material (e.g. Examination Papers) are held securely in the Academy safe and not opened until the examination. The only person entitled to access such material is the Examinations Officer.

Responsibilities

All staff must be aware of and adhere to this policy and procedure. The Act requires that all personal information is kept confidential and secure. Staff must therefore:

- Observe all instructions or directions given to you in respect of confidentiality and security of information;
- Comply with all security and confidentiality obligations contained within their employment contract;
- Keep workstations locked when away from desks and keep any documentation containing personal information out of sight overnight, not left out on desks;
- Inform the organisation of any changes to your personal details to enable us to comply with the Act and to aid the smooth running of the business;
- Keep all lockable cabinets and drawers in which personal information is stored locked when not in use; and
- Treat any documentation taken out of our offices in the same way as when in the office, ensuring security of information
- Information held must be accurate, relevant and not excessive. If staff need to hold or collect personal information they must therefore:
 - Ensure that all documents containing personal information are up to date and held for no longer than is necessary; staff should be aware that what constitutes "no longer than necessary" will vary and takes into consideration the type of information and the purpose to which it is to be put;
 - Ensure that all documentation or other materials no longer required containing personal information are disposed of via secure destruction bins / shredders; and
 - Ensure that the content of personal information held is objective; the information you hold may be disclosed to the individual concerned.



Staff must ensure that only the “authorised processing of information” takes place. In practice this means that:

- Information held and used must be required by staff in the course of their employment; staff must not access, gather or hold information which they do not genuinely need in order to carry out their role;
- Access to personal information should be refused to individuals both internally and externally (without the consent of the data subject), unless it is clear that these individuals are authorised to access or process such information (see Data Disclosure)

Except in certain limited circumstances, it is a criminal offence to obtain or disclose personal data or the information contained in personal data or to procure the disclosure of the information contained in personal data to another person without the consent of the person responsible for our compliance with the Act.

This means that:

- Staff may be committing a criminal offence if they do not process data in an authorised manner, whether done so deliberately or because of insufficient care;
- Staff must comply with the terms of this Policy and with any further instructions or directions given to you;
- If staff have any doubts or queries concerning access to, or use of, personal data in the course of their employment they should seek guidance from their Manager or any relevant Compliance Officer.

Data Disclosure

Disclosing information concerning members

1. It is not usual practice to discuss any member of the Academy without their permission. However, there are circumstances in which we would need to waive this agreement.
 - i. If a member of staff may believe a person will cause serious physical harm to others or to themselves. In these circumstances the member of staff would normally seek permission from the student to break confidentiality unless there are also good grounds for believing the person is no longer willing or able to take responsibility for his or her actions.
 - ii. Where possible this decision should only be made after consultation with their Head of Department or Student Services.
 - iii. Any breaking of confidentiality will be minimised as far as reasonably possible. Information will be restricted to what is pertinent to the immediate situation and to those who can provide help for the person’s needs.
2. There is a legal duty to protect children from harm. Social Service guidelines state: “Anyone who has cause for concern that a child may be suffering or likely to suffer significant harm must refer the matter to the Social Services. **’Harm may be physical, sexual or emotional abuse or neglect’.**

If a person provides information that gives good grounds for believing a child may have been harmed or will continue to be harmed we have a duty to protect the child. If the person were not prepared to inform Social Services we would do so. We would also encourage the person to seek appropriate help.



Protecting identities

We aim to protect the identities of and information concerning individuals at the Academy. This means we do not give names, addresses or details of person to any outside agencies, persons or Departments without their express permission. To ensure maintenance of such confidentiality the following procedures are regarded:

1. If an enquiry is made verbally, by letter, by e-mail or by telephone about a learner/staff member. We will inform the enquirer that we do not give out information concerning service users.
2. If an enquirer says s/he has the person's permission to enquire. We will ask him/her to have the person verify this before we give information in consultation with the person in question.
3. An enquirer may have a legitimate reason for requesting information, e.g. concern about the safety of a learner or another person; a criminal investigation, etc. In such cases everything reasonable must be done to check the authenticity of such a query (verify police identity by asking rank and number, telephone the appropriate station).
4. An enquirer may claim to know that a person is seeing us. We will not confirm or deny this and explain that this is our policy.
5. A colleague may express concern about a learner. In such circumstances confidential advice about the specific issue can be given but the learner not be named unless s/he has already given their prior permission. This ensures that confidentiality is not compromised and the colleague is provided with professional support and advice.
6. A parent, relative or guardian may request information about a learner. We respect the adult status of learners and do not give information unless they have given prior permission.
7. Learner information is used by Academy administrative staff in reports, statistics, staff development and supervision. Reports and statistics should not make individual learners identifiable unless they have given prior permission. The presentation of 'casework' in reports or training sessions should protect client identity. Any major, detailed casework (e.g. case study for a training course or publication) should only be carried out with the clients' informed and expressed consent.
8. E-mails should be headed 'confidential' in the subject area. Where possible an individual should not be named in e-mail and circulation restricted only to those involved in resolving a particular problem.
9. To e-mails should be added a 'notice of confidentiality'. For example:

"This transmission is intended for the named addressee only. It contains information which may be confidential and which may also be privileged. Unless you are the named addressee (or authorised to receive it for the addressee) you may not copy it or use it or disclose it to anyone else." Or "Delete after reading".
10. Reports and letters should be written with the learner's permission. These to be headed 'confidential' and addressed to named individuals.



Learners' Rights

1. All users of student services have the right of confidentiality as stated.
2. Discussion and clarification of this confidentiality policy will be welcomed by support staff
3. Learners have the right to raise any breaches of confidentiality with the appropriate service and with Student Services.
4. Learners may seek support and advice from the Students' Union should they wish to pursue a formal complaints procedure.

Disposal of Information

Information will be held for a period of five years after the individual concerned has ceased association with the Academy. All digital information will be moved to a second secure location with access limited to the Director and all paper-based documentation will be shredded and disposed of safely. Where a third party (Legal requirement, particular awarding body etc) requires retention for periods in excess of this, the specific requirements of the said organisation will be taken into account. Any attempt to misuse or disclose such information to unauthorised parties will result in legal action being taken against the parties concerned

Staff training

Staff responsible for the management of personal data must have had training in the provisions of the Data Protection Act 1998. All staff working with personal data need to be reminded that it is a disciplinary offence to disclose confidential information to unauthorised individuals.

References

Providing a reference involves the disclosure of personal data of the individual who is the subject of the reference. So that we can ensure we protect our employees' data no references (whether to prospective employers or other institutions) should be given on behalf of the organisation without prior authorisation from the senior person. This Policy does not prevent any employee giving a reference in a personal capacity but employees should make clear that such references are personal and not on behalf of the organisation and, if the reference is given on paper, that neither the organisation's name, address nor logo appear on the paper. It is our policy to provide copies of references given by us to the individual who is the subject of the reference if they request a copy.

Marketing Activities

City College of London will also comply with the terms of the Act and with other relevant legislations such as the Privacy and Electronic Communications (EC Directive) Regulations 2003, in relation to its marketing activities. Direct marketing refers not only to selling products and services to individuals, but also includes promotional activities. All individuals, without exception, have the right to prevent or stop their personal information being used for direct marketing. City College of London will state how personal information will be used and how individuals will be contacted. We will inform individuals how and by whom their information will be used. This will include telling them that information may be shared with other organisations with similar aims and objectives. When we collect information from people and are in direct contact with them such as in a phone call or via our website, we will provide an immediate opportunity for them to opt out of further contact and to let us know how they would like to be contacted.



We will not:

1. Make unsolicited **phone calls** to any organisation or individual who has told us they do not want our calls, or to any number on the Telephone Preference Service list.
2. Send unsolicited marketing by **electronic mail** to individuals without first getting their permission.
3. Send unsolicited **fax** marketing to anyone who has a number on the Fax Preference Service, or who has told us they object.

In all our marketing we will identify who we are and provide contact details so that the recipient can contact us. If an individual decides they no longer want to receive marketing, we will deal with their request promptly and courteously.

Public Information Reliability & Communication Channels

City College of London is responsible for ensuring that its public information is accurate, complete and up-to-date. Information about the Academy its courses for those considering joining the Academy is made available to an audience both in the UK and overseas and the primary means of distribution is through the website www.utopiaacademy.co.uk Additionally, for enrolled learners the Academy publishes various policy and procedure documents and guidance handbooks via its intranet platform (CRM), much of which is also available in hard copy from the Administration Office.

Public information in this context means information in the public domain about academic standards and the quality of learning opportunities available at City College of London. This includes information available to its learners (both current and potential) and staff as well as all other public bodies.

Information displayed in City College of London's literature may have been supplied by an external organisation such as the Academy's accrediting body or an awarding body, but the majority of content will have been produced and published by the Academy itself. The Academy is however, responsible for all such content and has therefore implemented procedures for ensuring that the information that it has published about itself is accurate and complete. These procedures have been designed to ensure that City College of London:

- Recognises all the information that it is responsible for publishing
- Has rigorous mechanisms for the management of these responsibilities
- Can supply evidence that this is the case

In broad terms the type of information that procedures have been designed to manage are:

- General contextual information about the institution
- Information about the academic standards and quality of programmes

Communication channels/documents for the dissemination of this information typically include:

- Website
- Intranet (CRM)
- Prospectus
- Publicity materials (inc advertisements, leaflets, posters, HotCourses.com, etc.)



- Social media (Facebook, Twitter, etc.)
- Student handbooks
- Programme specifications and module descriptors
- Quality assurance documents
- Policy documents
- Strategy documents
- Monitoring and review documents
- Quality rating reports by students (feedback from surveys)
- External references (e.g.):
 - o Audit reports from accrediting/awarding bodies
 - o Progression agreements with universities

Completeness and accuracy procedures

Pre-enrolment

City College of London has procedures in place for ensuring that the information it puts into the public domain is accurate and complete.

Marketing and publicity material is initially typically drafted by the marketing team (see p9), and then circulated (if appropriate) to relevant course leaders (or they are consulted in person) or module tutors for comment on accuracy and appropriateness since team members, as professionals and experienced academics, often have a good understanding of the information needs of the market. The Principal will then check for accuracy and whether any associated external body needs to be consulted prior to publication (e.g. a university, a government body or an awarding or examining body, etc.). The draft material is then returned to the marketing team who make a final check to ensure text meets with any other publishing guidelines before returning it to the Principal for final approval.

Similarly the Admissions staff in conjunction with the Principal ensures that the prospectus, promotional material, advertisements, social media and the Academy's website information is complete, accurate and provides clear information to prospective students, parents/guardians and all other relevant third parties. Course entry requirements are clearly stated on the website and in course handbooks.

The Principal and Marketing Team review website content on a regular basis and annually update (or more frequent if required) according to the recommendations and action points derived from the awarding bodies, regulatory authorities and Academy management or other relevant party. Advertisements and other publicity materials can often be a one-off, so review is not always necessary. However where adverts are being re-cycled the copy should be approved again prior to publication.

Post-enrolment

Published information that relates largely to post-enrolment application is managed through the Principal and Director of Studies. This covers documents such as: Student handbooks; Programme specifications and Module descriptors and all relevant policy & procedure documents including: Quality assurance systems; Strategy documents and statements; Review reports and External agency references. The Principal may subsequently delegate specific responsibilities to either academic faculty (typically course leaders) or administrative staff for further scrutiny. Final drafts were then sent back to the Principal for approval and authority to publish.



External References

If content being published refers to arrangements in place with a collaborative partner, university, awarding body etc., copy text would be sent to the external body prior to publication for approval. In some circumstances, the external body (e.g. QAA, ISI) may issue the Academy with 'advertising and publishing guidelines that would clearly state what is or is not permitted, and in some cases also provide the acceptable wording for any references to their organisation and/or the relationship.

Monitoring effectiveness of publishing arrangements

The Admissions Office receives enquiries and applications on a daily basis, so is in a position to identify the effectiveness of the Academy's published material through verbal feedback taken at the time. In addition the regular issue of student survey forms solicit feedback on the accuracy of published information prior to enrolment and whether the course has met with expectations.

The Principal also works closely with the Admissions Office to ensure that all contextual information prepared for publishing is appropriate and relevant to the enquiry needs of the potential applicants/market.

Information made available to enrolled students via the Academy's intranet is easily accessible and serves as an essential reference point covering all aspects of their learning experience – including: programme specifications; assessments; appeals and complaints, careers guidance; student representation, etc. Again, the effectiveness of this content and its accessibility is measured through regularly conducting student feedback.

Representation

It is the aim of City College of London that its publicity material makes genuine effort to reflect the diversity of its demographic and the inclusivity of its policy and practice in accordance with its equal opportunities statement and welfare policy. To this end, it will avoid stereotypical or token images and will use clear and unambiguous language in all published media.

External Bodies

City College of London is registered with the Information Commissioner's Office (ICO) which oversees the framework for the responsible management of data including its collection, storage, distribution and disposal. All work conducted by the Academy is compliant with the guidelines issued by the ICO.

The Academy is also registered with the Copyright Licensing Agency (CLA). This enables the Academy to reproduce copyrighted material to facilitate the learning of its students. It also ensures that work produced by the Academy is considered intellectual property and is subject to the same conditions of reproduction by others.

Copyright Laws

Under copyright law it is illegal (for copyright protected software) to:

- Copy software/data
- Run pirated software
- Transmit software over a communications line, thereby creating a copy.

IT Usage

The Academy's internet connection is provided primarily for learners and staff to explore educational and research materials related to their course and Academy work. The use of the Academy's internet



is a privilege, not a right, and is provided for those who agree to act in a responsible way. Internet use is monitored and filtered by the Academy.

Usage of the Internet and E Mail

Users of the network will be issued with a login ID and a password. This will allow access to network files, secure storage space on the network, and other network resources such as printers. Individual login ID will allow access the users own private file area on the network, as well as shared file areas. Users should keep their login ID and password secure and must not disclose them to anyone else. Users must not use any other person's login ID or password or attempt to log into the network with any login ID other than the one that has been issued to them. Users should:

- Address colleagues in an acceptable manner using a salutation together with the name of the person to whom the message is directed, if the email is to a group of people then using the terminology of colleagues would be acceptable. The message should end with the senders contact details.
- Keep all user emails for urgent Academy work
- Keep email messages brief and to the point
- Avoid unnecessary copying or forwarding of emails, and use of blind copies
- Check their mailbox at regular intervals which helps ease congestion
- Always identify themselves when sending an email

Users may use the internet for purposes not directly related to work but **you must not do this during working time.**

Personal Use

The main purpose for the provision by the Academy of IT facilities for email is for use in connection with teaching, learning and approved business activities. The Academy permits the use of its IT facilities for email by staff, students and other authorised users for personal use, subject to the following limitations:

- Access only in own time i.e. before work, lunch break, after work
- A level of use that is reasonable and not detrimental to the main purpose for which the facilities are provided
- Priority must be given to use of resources for the main purpose for which they are provided
- Personal use must not be of a commercial or profit-making nature, or for any other form of personal financial gain
- Personal use must not be connected with any use or application that conflicts with the business of the Academy
- Personal use must not be connected to any purpose or application that conflicts with the Academy's rules, regulations, policies and procedures
- Personal use must comply with the Academy's policies and regulations, in particular the Email policy.

Prohibited Internet and Email Usage

Users are not allowed to:

- Contravene the Data Protection Act, such as the emailing or posting of confidential information.
- Send, display, print or download text, images, video or sound which is offensive or degrading to others based on any protected characteristics (refer to Equality and Welfare Policy)
- Send email chain letters.
- Use obscene, racist or degrading language in emails.
- Produce propaganda for religious or political causes.
- Break copyright laws, whether the Academy's or others' intellectual property.
- Try to enter a Academy or other computer system without permission (i.e. Hacking).
- Attempt to damage the Academy network or systems e.g. knowingly downloading files that contain malicious code such as a virus.



- Edit, move or delete any systems files or programmes already installed on the system.
- Play or download PC games or software from the Internet.