EMPIRE COLLEGE LONDON
INFORMATION SECURITY POLICY

Copyright © 2025 | Empire College London

1 PURPOSE & SCOPE

Empire College London (*hereinafter referred to as the **"College"***) collects stores and processes personal information about its students and members of staff. The College manages personal and sensitive information in both electronic and paper.

This policy is applicable to all data and information held within IT and paper-based systems, including but not restricted to: desktop computers, network servers, portable equipment, electronic data, paper files, hard copy and logs.

This policy informs staff and students of the way in which their personal information is handled and explains the obligations of the College, its staff and students under the Data Protection Law. One of the most important obligations is that personal information must be safeguarded against unauthorised or unlawful processing and against accidental disclosure, loss, destruction or damage. This means that the College, staff and students must take appropriate measures to ensure that personal information is kept secure with access strictly controlled and limited to those who are entitled to access it as part of their duties. This policy defines responsibilities of staff and students, for ensuring that any information they provide to the College is up-to-date and accurate and that they inform the College of any changes to the information they have provided.

2 POLICY

2.1 PROCESSING PERSONAL INFORMATION

The College must also take reasonable steps to ensure that staff, students and other users of the College's facilities do not pose a threat to the health and safety of others. Accordingly, the College will process personal information as it requires in order safeguarding those to whom a duty of care is owed. This may include obtaining information about staff and students from third parties.

Staff and Students should ensure that the College is made aware of any medical condition along with relevant information about their medication. This information will be used to protect their health and safety and the health and safety of others.

2.2 CLASSIFICATION

The classification of data and information will be carried out according to the following guidelines:

- **Unrestricted:** Public information (including information deemed public by legislation). Information in this category can be made freely available the public, all staff and students.

- **Protected:** Information that is sensitive outside the College and needs to be protected. Authorized access must be granted by the appropriate manager to this information on a 'need to know' basis for business related purposes.

- **Confidential:** Information that is sensitive within the College and is only available for a

Copyright © 2025 | Empire College London

specific business function, group or role.

- **Restricted:** Senior Management Team will have the authority to access any highly sensitive information within the College.

3 INTEGRITY OF DATA

All users of College ICT systems are responsible for the integrity of information and data under their control.

Staff and Students should only access systems for which they are authorised. Access privileges will be modified or removed, as appropriate, when an individual changes or leaves their employment at the College.

Any information both electronic and hard copy, to be shared or used outside of the College which contains personal or sensitive information must be covered by an appropriate Protocol, ensuring compliance with Data Protection requirements. Any member of staff submitting electronic information to external partners under the arrangements agreed in a Protocol must ensure that files are fully encrypted, or password protected and that notification of passwords is secure.

No College data or electronic documents containing sensitive information that would damage the reputation of the College or expose the College to legal action should it be lost, may be transmitted electronically, copied to removable media or portable devices without the express written consent of a Data Protection Officer. Under no circumstances may non-encrypted sensitive data be removed from College premises either physically or by electronic transmission. Failure to comply may lead to disciplinary action.

Staff members must not disclose personal information to any third party, or even to the person to whom it relates, except in accordance with this Policy and the College's authorised procedures.

The College reserves the right for appropriately authorised staff to examine any data including personal data held on College systems or, when operationally necessary, for example to give supervised access to a private account to a colleague. Certain staff within the College have been authorised to examine files, emails and data within individual accounts, but will only do so when operationally necessary.

When a member of staff leaves the employment of the College their user account(s) shall be ended as part of the termination action carried out by the College. Thereafter, the College has the right to access the account for operational reasons and for the continuing delivery of services.

Prior to staff's termination of contract, managers should ensure that:

- All IT assets are returned to the College (e.g. laptops, mobile phone devices)
- Staff does not inappropriately wipe or delete information from hard disks. If the circumstances of leaving, make this likely then access rights should be restricted to avoid damage to College information and equipment

Copyright © 2025 | Empire College London

No external party shall be given access to any of the College's key systems unless that party has been formally authorised by an appropriate Manager. Prior to access being granted they will be required to adhere to the College's ICT Equipment Acceptable Usage Policy.

If temporary passwords need to be issued to allow access to confidential systems these need to be disabled when the visitor has left. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation from the relevant manager.

Key safety procedures to be observed at all times are:

- Staff accounts are rendered inactive when they cease to be employed by the College. Student accounts are rendered inactive and deleted at the end of each academic year.

- Passwords are the responsibility of individual users and must be kept confidential. The passing of an authorized password to someone unauthorized in order to gain access to an information system is a disciplinary offence.

- The College network perimeter must be protected by a firewall and internet access controlled through a web filtering device.

- Anti-virus protection software must be installed on all of the College devices. If a user believes that his/her device is not protected, then he/she must contact IT Manager immediately. Users should report any viruses detected/suspected on their equipment to IT Manager.

- All College devices shall be controlled to prevent the installation of malicious or fraudulent software/code.

- The loading and use of unlicensed software on College devices is not allowed.

- Key business systems shall be protected by an additional level of user access control.

- It is the responsibility of the IT Manager to ensure that access rights and control of traffic on all College networks are correctly maintained.

- It is the responsibility of the IT Manager to ensure that data communications to and from remote networks and computing facilities do not compromise the security of the College ICT systems.

- All hard copy of staff, student, financial, research and business records should be stored in a secure area and not left in an unattended, unlocked room. They should only be retained for the minimum length of time that they are absolutely or legally required.

Copyright © 2025 | Empire College London

4 Access to Information

Subject to limited statutory exceptions, all staff and students are entitled to know what information the College processes about them and why.

Any person who wishes to exercise their right to view information held about them by the College should apply in writing. Students and staff should write to the Data Protection Officer with proof of their identity and details of the information they wish to see.

The College will aim to comply with requests for access to personal information within 30 days of receipt of the request but may require longer in certain circumstances. In such cases, the College will contact the individual to explain the reasons for the delay.

Access will not necessarily be given to the following types of information:

- References given to third parties by the College.
- Management information where disclosure would prejudice the College's business planning.
- Information which would affect ongoing negotiations with the person who requested access. Confidential information, disclosure of which would reveal the informant.
- Information which identifies third parties where those third parties have not given consent to disclosure (subject to exceptions).

Refer to the Subject Access Request Procedures for more information.

5 Physical Security

Controls are implemented as appropriate to prevent unauthorised access to, interference with, or damage to, the College's key ICT systems. Key physical security procedures to be observed at all times are:

- File servers and storage arrays facilities shall be controlled and restricted to authorized personnel.
- Key ICT Infrastructure shall be housed in secure, locked racks.
- All ICT infrastructures shall be managed by IT Manager and cannot be worked on or accessed without the authorization of the IT Manager.
- Personal ICT equipment may only be connected to the college ICT systems over public wireless SSID's. Personal ICT equipment shall not be allowed to participate in domain membership and will only be granted guest access to available services.
- No hard wired connections shall be made to the College ICT Systems without the authorization of the IT Manager.

Copyright © 2025 | Empire College London

- Users of College ICT facilities are responsible for safeguarding key data and equipment by ensuring that desktop machines are not left logged-on when unattended, offices and classrooms are kept locked and that portable equipment is not exposed to opportunistic theft.

- Users must log off the computer network or initiate a password-protected screensaver when leaving a workstation unattended to prevent anyone else accessing the network using their security credentials. A member of staff or student that fails to do this will be deemed to be the person accessing the network unless it can be proven otherwise.

- Users of portable equipment belonging to the College are responsible for the security of the hardware and the information it holds at all times on or off College property. The equipment should only be used by the College staff to which it is issued and should be secured when not in use.

- Users must contact the IT Manager if they are aware of or suspect a security breach.

- Any computer or mobile device that is perceived to be placing the integrity of the College's ICT network at risk will be disconnected.

6 INTERNET

The internet is a pivotal part of the services offered by the College and as such, must be accessible to all staff members during their work hours. However, we recognise the security risks of using the internet and so access is only available through the College's local network or secured wireless network with the appropriate infrastructure and firewall protection. The internet is not permitted for personal use and certain sites are blocked by default to enforce this rule. The College have also restricted the sharing of files on certain systems and for some individuals, dependant on their need to use such facilities. All Internet access is monitored and logged. The College may suspend access to the Internet when it is deemed that there is a significant security risk to the College from external sources.

7 EMAIL USE AND GUIDELINES

Email is necessary for the service provision offered by the College and is afforded to all staff members. Email is accessible via secured connection. College has set out guidance for staff members on how to use email for legitimate purposes.

7.1 ACCEPTABLE USE

The College have adopted the below set of acceptable use guidelines for staff members to follow when using the College email: -

- Email must be used in accordance with current legislation and regulations
- Staff must adhere to this policy at all times when using college email

- Staff must only access their own college email and must not share or disclose logins or passwords
- Staff must report any unusual or flagged email messages to the IT Department immediately
- College email should only be used for legitimate business use

7.2 PROHIBITED USE

In addition to the acceptable use of the College email system, the below actions and forms of use are unacceptable and must be adhered by all staff members. ***College email must not be used: -***

- To send or receive inappropriate content or attachments, including distributing, disseminating or storing images, text or materials that might be considered indecent, racist, sexist, abusive, offensive, pornographic, obscene or illegal
- For personal use, to disseminate personal views or opinions or to access personal emails
- For sending confidential messages to any unauthorised person or location
- To sign-up to personal or inappropriate internet sites
- For sending or forwarding *'chain letters'* or social content
- Forwarding of college confidential messages to external locations
- To send, receive or access any copyrighted information in a way that violates or breaches that copyright
- To send unsolicited marketing or advertising material
- In a way that restricts the sending or receive of files by other staff members *(i.e. sending large files without pre-authorisation)* or for undertaking deliberate activities that waste any networked resources
- In a way that could introduce any form of computer virus or malware into the College network

7.3 EMAIL SECURITY

The IT Department is responsible for ensuring that the network and email system is adequately protected from viruses and malware. However, users can also help in avoiding security issues by complying with the below responsibilities. ***Users of the email system must not: -***

- Send or open any attachment that is not recognised, authorised or has come from an unknown source
- Alter any of the security settings on the device being used to access the email system
- Send any personal or confidential information. Speak to the IT Department who will advise on the correct secure transfer tool or system for the file type
- Disclose your email login or password or attempt to access another user's email system
- Leave email systems open, unattended and unlocked when leaving a desk or the room

Copyright © 2025 | Empire College London

The email system is the property of the College and all emails sent and received, including by remote access, may be subject to access and monitoring by the College both during and after users' employment/enrolment at the College. The College may also delete messages or suspend email services to prevent or restrict the flow of messages at its discretion.

8 REMOTE ACCESS

Specific staff may be granted the capability to access the College's computer network from outside the College's premises. The ability to do so is controlled by IT Manager who must first give express prior consent for remote access. Remote access requires the issuing of secure keys to the user. These keys must not be revealed to anyone or used to remotely connect any other machine/device other than that of the user to whom they are issued. The College reserves the right to terminate remote access and/or to change security keys without prior notification.

Staff who is able to access the College's computer network remotely must return to the College any materials, equipment or other items enabling such access upon ceasing their employment at the College.

9 TELECOMMUNICATIONS

The telecommunications system is the property of the College and any calls made to or from it may be subject to monitoring by examination of the system logs itemised telephone bills.

10 POST

Post received at the College's premises is the property of the College. If any post is received which is marked for the attention of individual staff it will generally not be opened prior to distribution. However, the College reserves the right to open and inspect all mail.

Staff and Students must not use the College as a personal mailing address.

Any mail received by the College for the attention of any learner or member of staff who is no longer a learner or member of staff of the College will be opened and dealt with by the College in whatever manner the College thinks fit.

11 CCTV

The College uses closed circuit television (CCTV) images to provide a safe and secure environment for students and staff and for visitors to the College premises and to protect the College property.

There are specific cameras which also record an audio stream; these are located in the college reception areas on the first and second floor; the primary purpose of audio recording is to detect any abusive and inappropriate behaviour towards staff and students. Clear signs are displayed, where audio recording in progress.

The purposes of installing and using CCTV systems include:

Copyright © 2025 | Empire College London

- To assist in the prevention or detection of crime or equivalent malpractice.
- To assist in the identification and prosecution of offenders.
- To monitor the security of the College premises.
- To ensure that health and safety rules and College procedures are being complied with.
- To assist with the identification of unauthorised actions or unsafe working practices that might result in disciplinary proceedings being instituted against students and staff and to assist in providing relevant evidence.

Cameras are located at strategic points throughout the College premises, principally at the entrance and exit points. Cameras only cover communal or public areas on the College premises, and they have been sited so that they provide clear images. No camera focuses or will focus, on toilets, staff break rooms or private offices.

All cameras (with the exception of any that may be temporarily set up for covert recording) are also clearly visible.

Appropriate signs are prominently displayed so that students, staff and other visitors are aware they are entering an area covered by CCTV.

11.1 RECORDING AND RETENTION OF IMAGES

Images produced by the CCTV equipment are intended to be as clear as possible so that they are effective for the purposes set out above. Images may be recorded either in constant real-time (24 hours a day throughout the year) or only at certain times, as appropriate.

As the recording system records digital images, any CCTV images that are held on the hard drive of a CCTV recorder are deleted and overwritten on a recycling basis. Once a hard drive has reached the end of its use, it will be erased prior to disposal. Images that are stored on, or transferred on to, removable media such as CDs are erased or destroyed once the purpose of the recording is no longer relevant. However, where a law enforcement agency is investigating a crime, images may need to be retained for a longer period.

11.2 ACCESS TO AND DISCLOSURE OF IMAGES

Access to, and disclosure of, images recorded on CCTV is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purposes for which they were originally collected.

The images that are filmed are recorded centrally and held in a secure location. Access to recorded images is restricted to the operators of the CCTV system.

Disclosure of images to other third parties will only be made in accordance with the purposes for which the system is used and will be limited to:

- The police and other law enforcement agencies, where the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness.
- Prosecution agencies, such as the Crown Prosecution Service.

Copyright © 2025 | Empire College London

- Relevant legal representatives.
- Senior Managers involved with College disciplinary processes.
- Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).

The Data Protection Officer (or another senior manager acting in their absence) is the only person who is permitted to authorise disclosure of images to external third parties such as law enforcement agencies.

All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

11.3 Covert Recording

College will only undertake covert recording with the written authorisation of the Senior Manager where there is good cause to suspect that criminal activity or equivalent malpractice is taking, or is about to take, place and informing the individuals concerned that the recording is taking place would seriously prejudice its prevention or detection.

Covert monitoring may include both video and audio recording.

Covert monitoring will only take place for a limited and reasonable amount of time consistent with the objective of assisting in the prevention and detection of particular suspected criminal activity or equivalent malpractice. Once the specific investigation has been completed, covert monitoring will cease.

Information obtained through covert monitoring will only be used for the prevention or detection of criminal activity or equivalent malpractice. All other information collected in the course of covert monitoring will be deleted or destroyed unless it reveals information which the College cannot reasonably be expected to ignore.

12 Storage, Disposal and Transmission

Controls are implemented as appropriate to ensure that physical devices and electronic media containing college data and information assets are protected from unauthorised access when in storage, being transmitted or transported and when disposed of.

Refer to the Date Protection Policy and Procedures for more information

13 Information on Desks, Screens and Printers

Members of staff who handle confidential paper documents should take the appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Copyright © 2025 | Empire College London

Care should also be taken when printing confidential documents to prevent unauthorised disclosure. Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended.

14 Removable Media

Removable media is any type of storage device or object that is physically able to be disconnected and removed from a system or computer whilst it is active. Such media types include, but are not limited to USB's, Media Cards, CDs, DVDs and SD cards.

Unless provided to a staff directly by the College, we prohibit the use or possession of any removable media devices on-site. Removable media devices pose a serious risk to the information held by the College. All removable media devices and any associated equipment and software are only available through the IT Manager. Where removable media is used to store important, essential or personal information, this will be done so as a encrypted backup format and is never the sole location of such data.

College uses the latest virus and malware checking software on all assets to ensure that where removal media devices are being used, these are scanned are authorised prior to allowing access to any networks, systems or servers.

Contact Details:

Empire College London
Forest House, 16-20 Clements Road, Ilford, Essex, IG1 1BA
info@empirecollegelondon.co.uk
Tel: 02085532683