UKMC IT Data Protection and Data Security Policy

Date	Author	Summary of Changes	Version	Authorised
March 2024	Head of IT	Revisions and appendix updates	2	Academic Board 24/09/2024
July 2025 / December 2025	Head of Quality and Compliance	Template reformatting. Role name changes. Inclusion of dataprotection@ukmc.ac.uk email address. Inclusion of AI data input and third-party risk compliance notes.	3	Academic Board December 2025
21/08/2026	Compliance Manager	Updates as per OFS requirements, also integration with Health and Safety, due to Safety concerns and risk profiling.	4	Q&S committee Pending EB Approval

Policy/Procedure Management and Responsibilities	
Policy/Procedure Owner	The policy is overseen by the Head of IT and approved by the academic board. Day-to-day implementation and communication responsibilities are delegated to relevant stakeholders within the IT Department, Data Protection Officer, and delegated nominees within UKMC.
Equality Impact / Analysis	Equality Impact Assessment completed and reviewed in accordance with UKMC policy governance requirements.
Authorised By	Academic board December 2025
Effective From	December 2025
Next Review	December 2028 or sooner where legislative, regulatory, cyber security, or organizational changes require review.
Version	4
Internal/External	Both
Document Location	UKMC | Policies and Legislation
Linked Documents	Data Protection Act 2018.

	Data Protection and Freedom of Information Fees Regulations 2004 Freedom of Information Act 2000 Environmental Information Regulations 2004 Privacy and Electronic Communications Regulations 2011 UKMC Code of Practice for Managing Freedom of Information Requests
Dissemination Plan	Public availability on the UKMC website. IT training, GDPR, staff training, embedding in bulletin and communications.
Accessibility	**Alternative formats on request. Email Quality@ukmc.ac.uk**

Purpose

1. This document defines UK Management College's (UKMC) policy on data protection and data security and is based on the following principles:

    1. UKMC will process personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (as amended), the Privacy and Electronic Communications Regulations (PECR) where applicable, and other relevant UK legislation.
    2. Ensuring compliance is a corporate responsibility of UKMC requiring the active involvement of, and appreciation by, all staff at all levels of the organisation.
    3. UKMC will strive to ensure best practice with regard to data protection and data security processes and procedures.
    4. UKMC will strive to improve practices and procedures using external guidance, monitoring of jurisprudence in the relevant areas, and adopting examples of best practice elsewhere.
    5. UKMC will provide support and services to enable staff handling personal data to remain compliant with the legislation and the Institution's requirements in respect of data security.

Introduction

2. At UKMC, personal data are held about students, staff and the public. The Institution needs to hold information about its students and staff for reasons which include, but are by no means limited to, the following:

    1. the recruitment of students;
    2. the recruitment, employment and payment of staff;
    3. the administration of courses and assessment of student work;
    4. student welfare.

Data may also be held on other individuals, such as enquirers to courses, visitors to the College, suppliers, employees of other organisations who are involved in the delivery of college courses, research activities and so on.

3. The Data Protection Act 2018 (DPA) places responsibilities and obligations on organisations which process data about living individuals. It also gives legal rights to individuals in respect of personal data held about them by others. The DPA may be found on the internet at https://www.gov.uk/data-protection.

4. The College is required to have policies and procedures in place to ensure compliance with its obligations under the Act that extend across its students, staff and the activities of the Institution.

Scope

5. This policy applies to UKMC personal data processing concerning applicants, students, staff, former staff and students, visitors, suppliers and other individuals, wherever processing occurs and regardless of whether information is held electronically or in paper form.
   1. All students studying at UKMC, including applicants to its courses and recruitment agents.
   2. All staff employed by the Institution.
   3. It applies to individuals and organizations accessing or processing UKMC information on UKMC's behalf, subject to applicable contracts and legal obligations.
   4. All institutional activities that involve the processing of personal data as defined by the Data Protection Act 2018.

Definitions

6. The following definitions apply to this policy:

   1. UK GDPR and DPA 2018: The UK GDPR and the Data Protection Act 2018, as amended, are the principal UK legal framework for processing personal data.

2. Personal data breach: A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
3. **Data subject:** A living individual who is the subject of personal data.
4. Data controller: The body determines the purposes and means of processing personal data. UKMC acts as a controller where it makes these decisions; arrangements for joint control or processing on behalf of other controllers must be assessed case by case.
5. **Data processor:** Any person or persons that process information on behalf of a data controller.

6. Personal data: Information relating to an identified or identifiable living individual, including relevant digital and paper records.

7. Information Commission (ICO): The UK supervisory authority for data protection. UKMC will maintain any required data protection fee registration and cooperate with regulatory enquiries as required by law.
8. **Information life cycle:** The time span that information processed by the College remains 'live' and relevant to the Institution (inclusive of its disposal or destruction) and for which the Institution has obligations under this, or any other policy.
9. Personal data may identify an individual directly or indirectly, including when combined with other reasonably available information. Pseudonymized information remains personal data where individuals can be re-identified.
10. **Processing:** An action of any sort taken in regard to personal data during the lifecycle of that personal data. This will include but is not limited to obtaining, storing, adapting, transferring, transmitting, disposal and destruction.
11. **Relevant filing system:** Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria

relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

12. Special-category data: Information within Article 9 UK GDPR (including health, race, religious beliefs, biometric data used for identification and trade union membership). Criminal-offence data is subject to separate Article 10 and DPA 2018 requirements.
13. Subject Access Request (SAR): A request by an individual to exercise their right of access under Article 15 UK GDPR. Requests may be made verbally or in writing; a particular form is not mandatory. Identification and clarification may be requested only where justified under applicable law.

Aims

7. The aims of the Data Protection and Data Security Policy are to:
    1. Set out the obligations of the Institution with regard to data protection and data security.
    2. Establish the guiding principles for the Institution's actions in this area.
    3. Provide a policy framework to ensure local compliance with the DPA and the Institution's requirements in respect of data security.

Policy statements

Notification

8. UKMC will maintain any data protection fee registration required by law and keep appropriate records of its personal-data processing. A registration or fee payment does not, of itself, demonstrate compliance with UK GDPR.

Personal data held by the College

9. Data are collected from students at various stages. Examples include, but are not restricted to:

1. data on applications
2. enrolment and registration data
3. applications for financial aid
4. data held by the Student Academic Office (SAO) in connection with student welfare

10. Data are also added subsequently to students' records, for example:
    1. marks and progression statements;
    2. changes of address;
    3. final degree results;

    4. medical certificates;
    5. extenuating circumstances applications;
    6. payment of fee and debt status.

11. The Department of Human Resources collects data on staff and creates a personnel file for every member of UKMC staff. Some of this information will also be held by individual administrative units within the Institution. Such data will include:
    1. applications for posts at the College;
    2. terms of appointment;
    3. appraisal;
    4. promotions;
    5. leave records.

12. All staff and students should ensure that any information that they provide to the College in connection with their employment or study is accurate and up-to-date. The College has ultimate responsibility for ensuring the personal information it holds is accurate and up to date.

13. Upon graduation, some information is passed to the College Alumni Team to allow that body to contact graduates about College events, products, services and

for survey purposes. SAO also retain basic graduate student data regarding academic progress to verify awards and to provide a record of lifelong learning.

Processing obligations – general

Data Protection principles in general

14. UKMC will comply with the seven UK GDPR principles: (1) lawfulness, fairness and transparency; (2) purpose limitation; (3) data minimisation; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality (security); and (7) accountability. UKMC will take proportionate measures to demonstrate compliance with these principles.

Lawfulness, fairness and transparency

15. Before processing personal data, the relevant UKMC business owner should identify an appropriate lawful basis under Article 6 UK GDPR and ensure information provided to individuals is transparent, accurate and relevant to that processing.

1. Consent is only one lawful basis and must not be assumed to be necessary or valid for every activity. Where consent is used, the conditions for valid consent and withdrawal must be met.
2. Student processing may rely on different lawful bases for admissions, enrolment, teaching, assessment, funding returns, safeguarding, welfare and optional communications. The applicable basis and privacy information should be documented for the particular purpose.
3. Employee and applicant processing may involve contractual necessity, legal obligations, legitimate interests or other applicable grounds. UKMC should not rely on blanket employment consent where consent cannot be freely given.

4. Where special-category personal data is processed, UKMC must identify an Article 9 condition as well as an Article 6 lawful basis and meet any relevant DPA 2018 Schedule 1 safeguards. Criminal-offence information must have lawful authority and appropriate protections.

Integrity and confidentiality — security of personal data

16. UKMC will use technical and organisational measures appropriate to the risks to personal data, taking account of the nature, scope, context and purposes of processing and the available controls. This policy states required outcomes; implementation must be confirmed through supporting procedures and evidence.

1. ensure that the personal data is technically stored and handled in line with approved College data security policies and processes;
2. ensure that Institutional measures are in place to guard against unauthorised or unlawful damage or destruction of the personal data. Such measures could include: restricting access to the data to minimum number of persons possible; ensuring that all digital personal data is password protected wherever it may reside; ensuring that any personal data are not left 'in the open' either in paper form, or on a screen in digital form; ensuring that access to the area in which the personal data is stored is restricted to only those persons who need to be there, minimising the need for transfer of the data, if transfer is required; and ensuring that College data security protocols are in place and observed;
3. take steps to provide an adequate level of training in DPA and information security to anyone with access to the personal data, inclusive of anyone outside of the Institution that may have access to the data.
4. The policy owner retains organisational oversight; operational IT security controls are managed by designated IT personnel within their approved responsibilities. The DPO or data protection lead, where appointed, advises on compliance and independently monitors relevant privacy obligations.
5. Appendix 1 provides additional guidance on the secure use of mobile devices.

UKMC will determine whether appointment of a statutory Data Protection Officer is required under Article 37 UK GDPR and maintain suitable privacy expertise and contact arrangements. Any appointed DPO must have the independence, resources and reporting access required by law; this role is not automatically responsible for implementing every technical control.

Other processing obligations

17. Staff should ensure that personal data are:
    1. processed only for the purposes for which they were collected (note that simply holding data on file counts as processing);
    2. not disclose personal data without an appropriate lawful basis, verified recipient and necessary authorisation;
    3. relevant, accurate and up to date;
    4. adequate but not excessive for the stated purpose;
    5. disposed of as confidential material when they are no longer needed for the purposes for which they were collected and in line with College data retention procedures;
    6. not initiate a restricted international transfer without assessing the UK GDPR transfer rules, relevant adequacy regulations, safeguards or applicable exceptions.

Data sharing

18. Personal data may be shared only where the proposed disclosure has a lawful basis, is necessary and proportionate, and meets applicable transparency, security and contractual requirements. The relevant business owner must establish the relationship between the parties.

19. Sharing for statutory obligations, contractual purposes, safeguarding or other legitimate activities must be assessed against the relevant lawful basis, confidentiality duties and any specific legal restrictions. The fact that a disclosure may be permissible does not remove the need for proportionate controls.

20. Where a supplier processes personal data on UKMC's behalf, the Article 28 UK GDPR requirements for a written controller–processor contract apply, irrespective of whether sharing is one-off or ongoing. Controller-to-controller and joint-controller arrangements should be assessed separately and documented where appropriate.

21. The relevant business owner should involve the designated data protection contact and procurement/contract owner when assessing material data-sharing or processor arrangements. IT provides proportionate advice on technical security where relevant; legal/contractual decisions remain with appropriately authorised owners.

22. Personal data should be shared through approved channels with access limited to authorised recipients and protections appropriate to the information involved. The technical controls used for a transfer must be proportionate to risk and available in the approved systems.

23. Where it is legitimate to share personal data with external organisations, the following hierarchy of actions should be adhered to:

1. Data should be uploaded via a secure portal wherever possible; most organisations using this method publish details of security systems on their websites.
2. Where there is no secure portal, data should be transmitted electronically (for example, as files, databases, PDF files, images) over secure networks. These files should be encrypted and, if so, then email is acceptable for such

transmission. Where the transmission of large sets of data is unavoidable, IT Services can advise how this is best achieved.

3. Data should be accessed through the host information system directly (if working away from the office, this may be done via a remote connection).
4. If it is unavoidable to share paper copies of sensitive data, they should be mailed in securely sealed envelopes and sent by courier or registered post. An individual's personal data in the form of, for example, assessment results or letters of appointments, may be sent in sealed envelopes using normal postal systems.
5. Particular care should be taken when transmitting sensitive data to unfamiliar recipients. Wherever possible the authenticity of the recipient should be checked with a known contact at the recipient organisation.

References

24. Confidential references and examination information may be subject to specific statutory provisions and exemptions. Requests must be considered individually under current UK GDPR and DPA 2018 rules, with advice from the designated data protection contact where needed. UKMC must not apply a blanket exemption without assessing the facts.

Research

25. Personal data used for research, archiving or statistical purposes must have an appropriate lawful basis and applicable safeguards. Retention and any exemptions from individual rights must be evaluated under the relevant statutory conditions; research data is not automatically retained indefinitely or exempt from access requests.

26. Care should be taken if a key is retained which enables anonymised data to be decoded and therefore attributed to individuals. An appropriate level of care would exist if the key was only known to those individuals directly involved in the research, and kept securely, and separate from the usual location of the anonymised data.

Care should also be taken when students are conducting research involving personal data as part of their studies. In such cases, the College may be the Data Controller and responsible for the student's adherence to the DPA.

27. Many research projects involving human subjects must first be approved by an Ethics Group, and one of the conditions of such approval is that the advice of the Provost has been sought. As part of this role, the Provost may ask to see a copy of the research protocol.

Examinations and assessment outcomes

28. Requests concerning examinations, scripts, marks and examiner comments must be assessed under the current UK GDPR and relevant DPA 2018 provisions. Any applicable exemption or modified response period should be documented and applied on a case-by-case basis, rather than relying on historical timescales.

System and process assessment

29. Before introducing or materially changing processing of personal data, the responsible department should assess data protection obligations and consult the appropriate privacy and IT functions. A Data Protection Impact Assessment (DPIA) must be completed where processing is likely to result in a high risk to individuals, with prior consultation with the regulator where legally required.

Third-party processors and international transfers: Proposed new services handling UKMC personal data should undergo proportionate legal, privacy and security review. Processor contracts and permitted overseas transfer arrangements must be in place where required. Procurement and business owners retain responsibility for obtaining appropriate approvals, with IT providing technical input where requested.

Cloud and Microsoft 365: Personal data must be processed in approved organisational services with appropriate access permissions, sharing controls, logging, retention, resilience and incident-response arrangements based on risk and actual system capabilities. This policy does not certify a specific Microsoft 365 or Azure feature as deployed.

AI and automated processing: Staff must not enter personal, confidential or restricted College information into unapproved AI services. Use of AI involving personal data should be assessed for lawful basis, purpose, provider terms, retention, international transfers, potential model training, transparency, security and DPIA requirements. Decisions having legal or similarly significant effects require applicable safeguards and human oversight where required by law.

Monitoring and surveillance: Any monitoring of staff, students or users, including CCTV, communications, audit logs and endpoints, must have a documented lawful purpose, proportionate scope, appropriate transparency and restricted authorisation. The separate CCTV and applicable employee privacy policies should determine operational detail.

Data protection rights and complaints: Appropriate channels should support access, rectification, erasure, restriction, objections and other applicable individual rights, with decisions, exemptions and timelines documented. Individuals may contact the UK supervisory authority in accordance with applicable law.

Direct marketing and electronic communications: Promotional emails, texts, cookies and similar technologies should be assessed under PECR and UK GDPR as applicable. Required notices, consent and opt-out arrangements should be established by the business owner before deployment.

30. Where advice and guidance is given, every opportunity will be explored to expand the knowledge and awareness of the individual or organisational unit seeking the advice and guidance.

Records and accountability: Where required, UKMC will maintain records of processing activities (ROPA), identify relevant information owners and periodically review the accuracy of records, notices and processor arrangements.

Privacy by design and default: UKMC should integrate data minimisation, appropriate access, retention, security and transparency into the design and change-management of systems and processes, with accountable business owners and risk-based review.

Training and awareness

31. Training and awareness is essential for UKMC to be in a position to meet its obligations under the Act.

32. The Director of Operations has primary responsibility for ensuring that adequate and appropriate training and awareness exist within the Institution, working closely with the Head of HR and the Provost.

33. Staff will receive data protection information appropriate to their role during induction and periodic awareness activity, coordinated through relevant College functions. Completion and effectiveness should be evidenced through proportionate records where training is mandatory.

34. The Director of Operations has overarching responsibility for the creation and maintenance of web-based and print material for reference and awareness. This post is also responsible for ensuring that scheduled training is available to staff and students and providing ad hoc training where appropriate.

35. The Director of Operations, in conjunction with the College Executive Board, will identify those roles requiring particular training and awareness of data protection responsibilities and will work with the relevant teams to ensure that adequate and appropriate training is provided. Monitoring of the effectiveness of training and awareness activities should be undertaken and maintained consistently.

Data breach management

36. All staff and relevant third parties must report suspected personal data breaches without undue delay using the approved IT/security or data protection reporting channels, so that containment, risk assessment and statutory deadlines can be considered promptly.

37. The responsible incident-response personnel should take proportionate steps to contain and investigate suspected breaches, preserve appropriate evidence, and consult the designated data protection contact regarding the risk to individuals and notification duties.

38. Where a personal data breach is notifiable, UKMC must notify the Information Commission without undue delay and, where feasible, within 72 hours after becoming aware of it, unless the breach is unlikely to result in a risk to individuals' rights and freedoms. High-risk breaches may also require notification to affected individuals without undue delay, subject to applicable exceptions.

39. The general procedure in the case of a data security breach will follow ICO guidelines and focus on the proper completion of four stages of breach management:

1. Containment and recovery
2. Assessment of on-going risk
3. Notification of breach
4. Evaluation and response

40. UKMC will document personal data breaches, including relevant facts, effects, remedial actions and reasons for notification decisions. Notification decisions and external communications must be made by appropriately authorised personnel, supported by specialist advice where appropriate.

Data Subject Access Requests (SAR)

41. A person may request access to personal data concerning them through any appropriate channel, including verbally or in writing. Staff receiving an apparent request should promptly direct it to the designated data protection contact; using a standard form is optional.

42. UKMC will ordinarily respond without undue delay and within one month of receipt, subject to lawful extensions or pauses where applicable. Reasonable identity verification, clarification and proportionate searches should follow current ICO guidance. Requests and decisions must be recorded and appropriately protected.

43. Detailed searches, disclosure checks, third-party redactions, exemptions and response approval should follow the current UKMC SAR procedure, where adopted. If no current approved procedure is available, the designated data protection contact should coordinate a legally compliant case-by-case response.

Data storage, retention and disposal

44. UKMC will apply security arrangements proportionate to risks arising from personal data, including access management, authentication, encryption, secure sharing, resilience, patching, endpoint protection and recovery arrangements where appropriate to the system and information concerned.

1. Data recovery arrangements, backup scope and restoration responsibilities are governed by the relevant approved backup and continuity documentation. This policy does not assert that every corporate system is backed up nightly or that a particular recovery time is guaranteed.

2. Access to UKMC networks, systems and cloud services should be limited to authorised users and controlled through applicable identity, endpoint and network-security arrangements.
3. Physical access to areas containing sensitive equipment or records should be restricted proportionately to the risks.
4. The login gives access to the College network. Both staff and students are advised to change their passwords immediately if they believe their details have been compromised.
5. Although workstations automatically lock if left inactive for a specific period, users are advised to always lock their workstations when moving away from their desk (windows key and L on a PC).

47 B. Data Protection and Security Controls:

USB Device Restrictions

1. Control objective:

- Prevent unauthorized data transfers and reduce the risk of malware entering organizational systems.
- Access to USB devices used as storage media is restricted on organisational computers to prevent unauthorised programs from running through removable devices and to reduce the risk of sensitive data being copied or transferred without permission.

The IT Department will:

- Restrict USB storage access through approved device-control settings.
- Prevent or limit the execution of unauthorized programs from removable storage.
- Permit exceptions only where there is a legitimate business or educational requirement and appropriate IT approval.
- Ensure any approved removable media is checked and handled securely.
- Investigate suspected misuse of USB devices or unauthorized data transfers.

- Users must not bypass USB restrictions or use personal storage devices to transfer organizational information without authorization.

2. Network Content Filtering

- Control objective: Reduce exposure to malicious websites and unsafe online content.
- Appropriate network or endpoint web-filtering may be used, where implemented, to reduce exposure to known malicious or high-risk online destinations. Coverage and effectiveness should be evidenced separately.

The IT Department will:

- Maintain appropriate web-filtering rules and security configurations.
- Block access to known malware distribution sites, phishing websites and other harmful destinations.
- Review filtering configurations and security alerts periodically.
- Investigate reports of inappropriate or unsafe websites that are not being blocked.
- Apply filtering and monitoring arrangements appropriate to the educational environment and relevant DfE requirements.
- Filtering exceptions must be formally authorised and assessed for security risks before implementation. Filtering controls must not be disabled or circumvented without approval.

3 Data Loss Prevention (DLP)

- Control objective: Prevent unauthorised disclosure, copying or transfer of sensitive information.
- Data Loss Prevention (DLP) measures will be used, where implemented and supported by the organisation's systems, to help identify, monitor and restrict inappropriate movement of sensitive or confidential information.
- DLP controls should address information such as student records, staff personal information, financial data and other restricted organisational information.

The IT Department and DPO will:

- Define sensitive data categories and appropriate handling requirements.
- Apply available DLP policies to relevant email, cloud storage, endpoint and file-sharing services.
- Restrict unauthorised transfers of sensitive data to external recipients, personal accounts or unapproved storage locations where technically supported.
- Investigate DLP alerts and suspected data exfiltration incidents.
- Record approved exceptions and ensure they have appropriate authorisation.
- Review DLP rules periodically and adjust them to address emerging risks.
- Users must only share sensitive data through approved channels and with authorised recipients.
- Implementation note: The exact DLP technology, policy rules and enforcement status must be documented by the IT Department. This policy does not, by itself, confirm that a particular DLP product or control has been deployed.

4 Multi-Factor Authentication (MFA)

- Control objective: Strengthen identity verification and prevent unauthorised account access.
- Multi-factor authentication should be configured for systems and accounts based on risk and approved technical requirements. The permitted methods, coverage and any exceptions are defined in the relevant identity and access standard; this clause does not certify universal deployment.
- The IT Department will:
- Configure and maintain MFA for supported organisational accounts and services.
- Require users to complete the approved identity verification process.
- Support secure enrolment, device replacement and recovery procedures.

- Review authentication settings and investigate suspicious sign-in activity.
- Apply stronger authentication requirements to privileged and administrative accounts where appropriate.
- Users must never approve an authentication request they did not initiate. Suspected MFA fatigue attacks, unexpected approval requests or compromised authentication devices must be reported immediately.

5 BitLocker Drive Encryption

- Control objective: Protect information stored on computers against unauthorised access if a device is lost, stolen or accessed offline.
- Full-disk encryption should be applied to relevant supported organisational devices, where technically feasible and proportionate to the risk, with exceptions assessed and documented. Deployment status must be verified separately.

The IT Department will:

- Maintain BitLocker encryption on applicable organisational computers.
- Monitor encryption status and investigate devices that are not correctly encrypted.
- Store and manage recovery keys securely through approved administrative systems.
- Restrict access to recovery keys to authorised personnel.
- Verify encryption status when devices are deployed, reconfigured, repaired or retired.
- Users must not disable or circumvent encryption settings. Lost or stolen devices must be reported immediately.

6 Secure Student Records — EBS Tribal

- Control objective: Maintain the confidentiality, integrity and availability of student records.

- EBS Tribal is used as an approved system for managing student records. Access to student information must be restricted to authorised personnel who require it for legitimate educational or administrative purposes.
- The EBS team working with the relevant system owner, will:
- Support secure access to EBS Tribal and its associated infrastructure.
- Ensure user accounts and permissions are assigned according to approved roles and responsibilities.
- Remove or amend access promptly when a user's role changes or access is no longer required.
- Protect administrative credentials and apply MFA where supported and required.
- Maintain appropriate system updates, security monitoring and backup arrangements in accordance with the agreed service responsibilities.
- Investigate suspected unauthorised access, alteration, disclosure or loss of student records.
- Ensure student information is accessed, stored and shared only through authorised processes.
- Student records must not be exported, copied or shared outside approved systems unless there is a legitimate purpose and appropriate authorisation.
- Access to student records must also comply with applicable data protection requirements and the organisation's student information handling procedures.

7 File Type Restrictions and Application Control

- Control objective: Prevent unauthorised software execution and reduce the risk of malware infection.
- Application execution and installation controls should be risk based and implemented through approved technical standards where supported. Exceptions must be assessed against business needs and security impact.
- The IT Department will:
- Maintain approved application and file-execution rules.

- Restrict unauthorised executables, scripts and other potentially harmful file types where supported.
- Prevent users from bypassing application-control restrictions.
- Review requests for additional software or file types before granting approval.
- Test changes to application-control rules to minimise disruption to legitimate educational and business activities.
- Maintain records of approved exceptions and review them periodically.
- Users must not run unauthorised programs, scripts or executable files downloaded from the internet, received by email or supplied through removable media.
- Any exception must be approved by the IT Department and implemented in accordance with the organisation's security procedures.

6. Access Control and Account Management with Geo Location

- Access to organizational systems and information must be granted according to the principle of least privilege.
- The IT Department will ensure that:
- Every user has an appropriately assigned account.
- Access rights reflect the user's role and operational requirements.
- Administrative privileges are limited to authorised personnel.
- Accounts are disabled or amended promptly when access is no longer required.
- Access permissions are reviewed periodically.
- Shared accounts are avoided unless specifically approved and appropriately controlled.
- Users must not share passwords, accounts or authentication codes with other individuals.

7. Geographical Access Restrictions

- Access to organisational systems, applications and information must be restricted according to the principle of least privilege and approved geographical access requirements.
- Authorised geographical access arrangements should reflect UKMC's operational needs, approved risk assessment and applicable information security requirements. No particular country restriction is established solely by this policy.

The IT Department will:

- Configure geographical access restrictions using available security controls, such as Microsoft Entra ID Conditional Access, firewalls or other approved security solutions.
- Apply geographical restrictions only where approved, supported and appropriately tested; technical configurations and approved countries or exceptions must be documented separately.
- Requests for additional geographical access should be approved by the appropriate delegated business authority under an agreed procedure, with IT responsible for technical assessment and implementation where authorised.
- Maintain a record of approved geographical access exceptions, including the business justification, authorised locations, duration and approval details.
- Apply approved exceptions only to the relevant users, systems and locations, and for the minimum period necessary.
- Review geographical access permissions periodically and revoke temporary access when it is no longer required.
- Monitor and investigate suspicious sign-in attempts originating from unauthorised geographical locations.
- Users must not attempt to bypass geographical access restrictions by using unauthorised VPNs, proxies or other methods.
- Requests outside any approved geographical access scope should be submitted through the agreed service or approval process before changes are made, except under authorised emergency procedures.

45. UKMC systems containing personal data should apply suitable access restrictions, security configuration and system ownership arrangements appropriate to the type and sensitivity of information.

1. Personal data should normally be stored in approved systems with access limited to those who need it. Locally stored information, exports and removable media should be minimised and subject to additional safeguards proportionate to the risk; specific configurations belong in supporting standards.

46. Personal data must not be retained longer than necessary for the relevant purpose, subject to applicable legal, statutory, contractual, regulatory, academic and preservation requirements. UKMC should maintain and approve a category-based retention schedule; no universal six-year retention period is imposed by this policy.

47. At the end of an applicable retention period, information should be securely deleted, anonymised or destroyed, unless a lawful preservation requirement applies. Business information owners are accountable for retention decisions, supported by IT for technical disposal and recovery considerations.

48. 51. Lost, stolen or damaged devices: Suspected loss, theft, compromise or damage of UKMC equipment must be reported promptly through the approved IT route and, where relevant, the line manager or HR. The incident should be assessed for information-security and personal-data-breach implications. Equipment care, investigations and any financial recovery are governed by the applicable separately approved asset/fair-usage and HR procedures. This policy creates no automatic employee liability or payroll deduction.

Complaints

49. UKMC will provide an accessible route for individuals to raise complaints about its handling of personal data. A complaint will be acknowledged within 30 days and considered appropriately, with the outcome communicated without undue delay. This does not prevent individuals from raising concerns with the UK supervisory authority. Appropriate contact details must be confirmed before publication.

Regulatory enquiries or complaints may be referred to the Information Commission (ICO): https://ico.org.uk/. UKMC should not require an individual to complete internal complaints steps before contacting the regulator.

Responsibilities

50. Within this policy, the following post-holders have these responsibilities:

Responsibility	**Owner**
Administration of subject access requests, response to data protection enquiries from students.	Director of Operations in liaison with the Provost
Initial investigation and management of data security breaches.	Director of Operations

Overall responsibility for Data Protection and Data Security Policy, authorization of actions related to data security breaches, raising awareness of DPA across the Institution, and the provision of training and information for staff and students	Director of Operations / accountable senior management (subject to confirmed governance arrangements)
Overall responsibility for those aspects of data security relating to UKMC information technology systems	Head of IT / delegated IT function — technical implementation and assurance, subject to agreed responsibilities
Strategic liaison regarding data protection and data security with the Executive and the Governing Body	Director of Operations
Institutional approval of Data Protection and Data Security Policy	Governing Body and Academic Board
Personal data to be handled in line with the College Data Protection and Data Security Policy, best practice and the Act	Staff and students handling personal data

Review

51. This policy should be reviewed at intervals established by UKMC governance and sooner following material legislative, regulatory, organizational or security changes. The Director of Operations, as recorded policy owner, should coordinate reviews with the designated data protection lead, Head of IT, HR, academic and other relevant stakeholders. Approval remains subject to the College's formal governance process.

References

52. The policy is supported within the context of the following pieces of legislation and UKMC policies:

ICO guidance: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/ (verify guidance current at formal approval).
ICO international transfers: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/.
UK legislation: https://www.legislation.gov.uk/ukpga/2018/12/contents and https://www.legislation.gov.uk/ukpga/2025/18/contents.

1. UK General Data Protection Regulation (UK GDPR); Data Protection Act 2018, as amended (including by the Data (Use and Access) Act 2025).
2. Data Protection and Freedom of Information Fees Regulations 2004
3. Freedom of Information Act 2000
4. Environmental Information Regulations 2004
5. Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), as amended, where applicable.
6. Applicable UKMC information governance and Freedom of Information procedures (titles and approval status to be verified).
7. Supporting UKMC IT, acceptable-use, remote-working, BYOD, CCTV, asset, security incident and business continuity policies, where formally adopted and applicable.

Appendices

53. The policy is supported by the following documents:
    1. Appendix 1: Secure use of mobile devices;
    2. Appendix 2: List of corporate system owners and administrators;
    3. Appendix 3: Staff data protection notice;
    4. Appendix 4: Student data protection notice;
    5. Appendix 5: Data Subject Access Request (SAR) Form;
    6. Appendix 6: Staff data collection consent – extract from College Contract of Employment (staff);
    7. Appendix 7: Student data collection consent – extract from Student Enrolment Form;
    8. Appendix 8: Data protection guidance for staff.

Appendix 1: Secure use of mobile devices

1. Purpose

This appendix outlines proportionate safeguards for mobile and remote devices used to access UKMC information. Specific configuration, ownership, BYOD and support requirements should be set out in the relevant approved device and remote-working standards.

This document should be read in conjunction with the Data Protection and Data Security Policy.

2. Definition

A mobile device is defined as a portable computing or telecommunications device which can be used to provide some of the functions typically associated with a desktop PC, such as storing or processing information. Examples include laptops, netbooks, tablets, smartphones, removable storage media (USB sticks/external hard drives) and wearable devices (Apple Watch/Pebble). As technology moves forwards this list is likely to expand.

3. Scope

All staff at the Institution including contractors, service providers and other organisations that use mobile devices to access College networks or information must comply with Institutional policy. It covers all mobile computing devices whether personally owned, supplied by the College or provided by a third party. Non mobile

devices that are not located on College premises and are used for accessing College networks or information are also in scope.

It does not cover personal devices of students at the College, only any device loaned to the student by the College, although it is suggested that students follow the policy to ensure the security of the data and information on their device.

4. Personally owned devices

Whilst the College does not require its staff to use their own personal mobile devices for work purposes, it is recognised that there is demand for this and it is often beneficial. The use of these devices is permitted subject to the following requirements and guidelines. Users must at all times give due consideration to the risks of using personal devices to access College data and information:

Requirements

1. An appropriate password/passcode must be set for all accounts on that device.
2. A password protected screen saver or screen lock must be used.
3. An appropriate screen lock should be enabled in accordance with the applicable approved device standard; the same interval need not apply to every BYOD platform.
4. The device must run the latest version of the operating system and be updated with software updates/security patches in a timely fashion.
5. Where a managed device supports approved location or remote-wipe capabilities, these may be used lawfully and proportionately with appropriate transparency. UKMC does not assume the capability exists for every personal device.
6. In the case of storage media all sensitive/confidential data stored on the device must be encrypted.

7. Any devices at risk of malware infection must run anti-virus software.
8. Any device used for this purpose should only be used by an authorised person. If family or friends are to use the device then it must be managed in such a way that others do not have access to this information.
9. Devices used for UKMC business should apply appropriate protection against unauthorised access, taking account of device ownership, supported management and the sensitivity of data. The detailed screen-lock interval should be set by an approved technical standard.

Where remote management, location or wipe capabilities are used, UKMC must ensure they are lawful, transparent, appropriately authorised and technically supported; these capabilities are not presumed to be available on every personal device.

10. Do not undermine the security of the device for example by Jail Breaking an iPhone.
11. Minimise the amount of sensitive/confidential data stored on the device.
12. If a device needs to be repaired, ensure that the company you are has an agreement in place which guarantees the security of any data on the device.
13. Do not leave devices unattended where there is a risk of theft.
14. Be aware of people around you when entering passwords or using the device.

5. College owned devices

The College will occasionally supply mobile devices to staff as required for their work. Where possible these devices will be configured in the same way as those which are permanently located on College premises. Occasionally it is not possible to configure the device for the user, and it will be the responsibility of the user to set the configuration.

Whether the device is configured by the College prior to release or not, the requirements and guidelines listed above should be followed and the following additional requirements apply to any College owned device:

1. Non-members of the Institution must not make any use of the supplied device.
2. No unauthorised changes must be made to the supplied device.
3. All devices must be returned to the College when they are no longer required or are in need of repair.

6. Third party devices

No staff should use any mobile device or other device that is for public use to access College networks or information. This includes public libraries or cyber cafes.

7. Lost equipment

Loss or theft of any device that contains or enables access to UKMC data should be reported without undue delay to the designated IT/security reporting channel so that relevant access and data risks can be assessed.

Appendix 2: List of corporate system owners and administrators

September 2024

System	System owner

Active Directory/Account Provisioning Service	Head of IT
External Examiners	Dean
Facilities Management	Director of Operations
Library Systems	Head of IT
Intranet/Applicant Portal	Head of IT
VLE	Head of IT
Finance systems	Director of Finance
Staff Systems	Head of HR
Student Records System	Head of IT
UKMC website	Head of Marketing

Appendix 3: Staff data protection notice

UKMC processes staff and applicant personal data for recruitment, employment administration, payroll, training, performance management, legal and other documented employment-related purposes under applicable lawful bases. A full, current staff privacy notice should state the relevant purposes, bases, recipients, retention, rights and contact details. This appendix is a summary pending confirmation of the live notice.

Disclosure of data

Data will be processed in accordance with the provisions of the Act and will only be disclosed within the Institution to members of staff who need to know it in order to carry out their duties, or to others connected with the College for College-related activities or events. Data will only be disclosed to a third party outside the Institution in accordance with the Act. This may include future employers who require verification of your period of employment.

Use of IT facilities

UKMC may undertake lawful, necessary and proportionate monitoring of its systems for documented purposes such as security, compliance and investigation. Monitoring is subject to appropriate transparency, access controls, authorisation and applicable staff privacy information.

Information provided to the Higher Education Statistics Agency (HESA)

Where UKMC is required or lawfully permitted to share staff data with statutory, sector or service bodies, the specific disclosures and applicable transparency details should be confirmed in the current staff privacy notice. This policy does not assume that submissions are fully anonymous.

Data retention

Employment records will be retained according to their category, lawful purpose and the approved retention schedule, with any legal preservation requirements applied as necessary.

Your rights as a Data Subject under the Act

Individuals have rights under UK GDPR, including access, rectification, erasure, restriction, objection and, where applicable, portability and rights relating to significant automated decisions. These rights are subject to statutory conditions and exemptions.

Your responsibilities as a Data User under the Act

You have three main responsibilities as a College employee with respect to the processing of personal data:

1. If you hold personal data in any form, whether on computer or in a manual file, as part of your job, this must be registered with your business unit in a form accessible by the Data Controller whose responsibility it is to ensure the Institution's data protection procedures are accurate and up-to-date. This includes any data that might be held by members of academic or academic-related staff for research purposes;
2. In dealing with personal data as part of your job, you must ensure that it is not shared with anyone other than individuals connected to College who need to know it in order to perform their work function. This covers both intentional disclosure and any disclosure that might happen by accident, for example through someone having oversight of your PC screen on which data is displayed. It is particularly important that personal details about members of staff or students are not given to anyone outside the Institution without prior consent of the individual concerned. If you are in any doubt, please do nothing until you have sought advice;

3. If you are a member of academic or academic-related staff, you are also responsible for ensuring that any students under your supervision who process personal data as part of their studies, for example in an undergraduate project or a postgraduate dissertation, conform to the requirements of the Act. Students who find themselves processing personal data as part of their studies are asked to contact their supervisor in the first instance; if you receive any such approaches please contact your line manager for advice.

Help and advice

Questions about staff personal data should be directed to the designated UKMC data protection contact, with HR involvement where appropriate. Confirm the operational contact before publishing the final notice.

Appendix 4: Student data protection notice

UKMC processes student personal data for admissions, enrolment, assessment, fees, welfare, statutory reporting and other identified educational activities under relevant lawful bases. The current student privacy notice must explain purposes, bases, recipients, retention, rights and contacts. This appendix is subject to verification against UKMC actual processing.

Specific disclosure of data

If you are involved in an emergency situation which results in you being hospitalised, the College may provide your emergency contact details to the relevant authorities dealing with the emergency, e.g. police, fire brigade or ambulance.

Disclosures to electoral-registration, local-authority or other public bodies should occur only where a current legal basis or statutory duty applies and should be accurately reflected in the relevant privacy notice; no routine disclosure is asserted here.

If you are registered at the College data is only disclosed to a third party outside the Institution in accordance with the Act. This may include prospective employers who

require verification of your qualifications, or other educational establishments if, at the end of your time at the College, you decide to undertake studies elsewhere.

Use of IT facilities

Any monitoring of IT facilities or communications must have a lawful and documented purpose, be necessary and proportionate, and be explained through appropriate privacy information and supporting monitoring controls.

Disclosure to statutory, regulatory, funding and sector bodies

Where applicable, UKMC may share student information with statutory, funding, regulatory, awarding or sector bodies under appropriate lawful bases. The current student privacy notice should identify relevant recipients and explain uses and rights; data must not be described as anonymous unless that can be substantiated.

Student survey disclosures and contact arrangements, where applicable, must reflect the current relevant bodies, survey programmes and UKMC's actual processing practices. Outdated references to HEFCE and historic survey programmes must not be reused without verification.

Any graduate outcomes or destination survey processing should be described in the current privacy notice, including who receives contact details, purposes, legal basis and how applicable rights are exercised.

You will have the opportunity to object to these contacts if you wish. Further details about the surveys and what happens to the information that is collected can be obtained from the Student Academic Office (SAO).

Data retention

When you leave, appropriate data is kept as a record to enable the College, if necessary, to provide references on your behalf, or to maintain a record of your academic achievements. The data is transferred to the College's record of its past students to enable us to keep in touch with you after you leave.

Your rights as a Data Subject under the Act

Students and applicants have rights under UK GDPR, including access, correction and other rights applicable to the particular processing, subject to statutory conditions and exemptions.

A request to exercise information rights can be made without completing a particular form. UKMC should respond through its designated privacy process within the statutory timeframe.

A subject access form may be offered as an optional aid, but it must not be a precondition for a valid request.

The SAO will be pleased to help with any queries you might have about any of your rights under the Act.

Your responsibilities as a Data User under the Act

It is unlikely that you will find yourself processing personal data as part of your studies at the College. However, if you do, perhaps as part of an undergraduate project, you will become a Data User under the terms of the Act and you will need to take certain steps to ensure that the College knows what you are doing and that your processing of data

conforms to the requirements of the Act. This does not apply to any personal data that you might hold for domestic or personal uses.

If you find yourself in this position, or are in any doubt, please see your Course Leader or Module Leader, in the first instance.

Help and advice

You may seek help and advice about the Data Protection Act, and how it affects you both as a Data Subject and as a Data User, from the SAO.

Appendix 5: Data Subject Access Request (SAR) Form

I, _____wish to have access to the data which the College currently has about me.

Please specify below

_____

_____

_____

_____

Signed _____

Dated _____

Appendix 6: Staff data collection consent

Extract from the College Contract of Employment for all staff:

DATA PROTECTION

UKMC employees must comply with UK data protection legislation and this policy. Staff personal data will be processed on an appropriate lawful basis for identified employment purposes and, where relevant, a separate condition for special-category or criminal-offence data. Acceptance of employment is not treated as blanket consent to all processing. The contract and current staff privacy notice should be reviewed by HR/legal before implementation.

Appendix 7: Student data collection consent

Data Protection Summary:

UKMC processes student data for identified education, administration, welfare, safeguarding, statutory and other lawful purposes. The current student privacy notice should explain the relevant lawful bases and any additional conditions for special-category information. Consent should be sought only when appropriate and valid.

Signing an enrolment declaration may acknowledge receipt of information or acceptance of applicable terms; it must not be described as consent to mandatory processing where another lawful basis applies. Any mandatory disclosure requirements should be stated transparently.

The College may release your personal data to third parties including current or potential employers, examination bodies, government departments or agencies or as otherwise required by law. Some examples of these are listed below:

1. Higher Education Statistics Agency – A statutory return for all Higher Education Institutions

2. Potential Employers – To provide a reference in relation to a job application

3. Current Employers – Where the employer is responsible for funding the course for a staff member, the College may confirm the status of the student on the course (current or withdrawn) and the results of any assessments taken
4. Under the terms of The Registration of the People (England and Wales) Regulations 2001, part III, paragraph 23 relevant data may be shared with the local Electoral Registration Officer
5. The Students Loans Company – to confirm attendance to enable payout of loan payments

6. Third-party cloud applications should be used only following appropriate approval and assessment of relevant security, processor, retention and international-transfer considerations. Named services must be confirmed as currently approved before inclusion in a published notice.

Appendix 8: Data protection staff briefing

All new staff to be given guidance during induction and updates provided at team meetings.

What does the Data Protection and Data Security Policy mean to you?

UKMC must protect personal data relating to students, applicants, staff and others through lawful, fair and secure processing. Staff must follow approved procedures, minimise unnecessary data sharing and promptly report suspected security incidents or breaches.

The UK GDPR provides rights for individuals and requires UKMC to demonstrate compliance with the seven data protection principles. The main obligations relevant to everyday work are summarised below.

- Maintain any required data protection fee registration and appropriate organisational accountability records.

- Process personal data in line with the seven UK GDPR principles:

  lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

- to answer subject access requests received from individuals. These may be staff, students or any individual who has an association with the College. They have important rights, including the right to find out what personal information is held on computer and most paper records.