King's College London Mathematics School Data Protection Policy

Monitoring and Reviewing

Action	Individual / Group	Date	Role
Reviewed	Dan Abramson	10/06/20	Head Teacher
Ratified	Finance and General Purposes Committee	16/06/20	Governors
Next review	Finance and General Purposes Committee	Summer 2022	Governors

1. Purpose

1.1. King's College London Mathematics School (KCLMS) collects and processes personal information belonging to applicants, students, employees, governors, contractors and others.

1.2. Maintaining the integrity and security of personal information, and ensuring its effective use for the intended purposes, is critical to the school's continued success.

1.3. This policy sets out to protect the 'rights and freedoms' of data subjects and to ensure that personal data is not processed without legal basis and processed only with their knowledge, wherever possible. It sets the standards by which personal information is managed by the school in order to ensure effective operation and compliance with relevant legislation in the best interests of data subjects.

2. Key personnel

2.1. Data Protection Officer

The Data Protection Officer for King's College London Mathematics School is Olenka Cogias, contactable at info-compliance@kcl.ac.uk

2.2. School contact

The key person responsible for Data Protection at KCLMS is Nicola Cosgrove, Business Manager, contactable at Nicola.Cosgrove@kcl.ac.uk

2.3. School contact

The governor with responsible for Data Protection is Page Starr, contactable via mathsschool@kcl.ac.uk

3. Definitions

3.1. Child

3.1.1. A natural person under the age of 13 years. Where no other legal basis applies, the processing of personal data of a child is lawful only with the consent of a person with parental responsibility.

3.2. Data controller

3.2.1. The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

3.3. Data Protection Officer (DPO)

3.3.1. The individual who assists the school in monitoring internal compliance, informing and advising on all data protection obligations, providing advice regarding Data Protection Impact Assessments and Data Breaches, whilst also acting as a contact point for data subjects.

3.3.2. The Data Protection Officer for King's College London Mathematics School is Olenka Cogias, who is part of King's College London's business assurance team.

3.4. Data Subject

3.4.1. Any living individual who is the subject of personal data held by an organisation.

3.5. Explicit consent

3.5.1. Consent obtained for the processing of specified personal data for a particular purpose.

3.6. Filing system

3.6.1. Any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

3.7. General Data Protection Regulation (GDPR)

3.7.1. EU regulation enacted in UK law as the Data Protection Act 2018.

3.8. Legal person

3.8.1. A non-human entity that is treated as a person for limited legal purposes, for example, a corporation.

3.9. Natural person

3.9.1. An individual human being, with consciousness of self.

3.10. Personal data

3.10.1. Any information relating to an identified or identifiable natural person ('data subject').

3.10.2. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.11. Personal data breach

3.11.1. A breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3.12. Processing

3.12.1. Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.13. Profiling

3.13.1. Any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour.

3.13.2. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

3.14. Special categories of personal data

3.14.1. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3.15. Third party

3.15.1. A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

4. Policy

4.1. Overview

4.1.1. KCLMS is committed to complying with the law in respect of personal data and the protection of the 'rights and freedoms' of individuals whose information it collects and processes. Its approach to compliance is described by this and associated policies, including the Staff Code of Conduct, the ICT Acceptable Use Policy, along with procedures relating to information security.

4.1.2. This policy applies to all functions which process personal data, irrespective of the data source. Data subjects include but are not limited to: learners, clients, employers, governors, employees, workers, contractors, volunteers, suppliers and other partners.

4.1.3. The Business Manager will conduct a biennial review of the Information Assets Register, and this review will be audited by the Data Protection Officer (DPO). Such reviews will take account of changes to the school's business operations and any additional requirements identified by means of Data Protection Impact Assessments (DPIAs). This register will be available to the Information Commissioner on request.

4.1.4. Adherence to this policy is required of all employees including casual workers, volunteers, contractors and governors of KCLMS. Potential breaches of this policy will be pursued in accordance with the KCLMS disciplinary proceedings and/or the terms of relevant contracts and other forms of agreement as appropriate.

4.1.5. Partners and any third parties working with or for KCLMS, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access or receive personal data controlled by KCLMS without having first entered into a data sharing agreement. Such an agreement must impose obligations on recipients which are no less onerous than those to which KCLMS is committed and must grant KCLMS the right to audit compliance with that agreement.

4.1.6. Where there is apparent potential for a criminal offence to have been committed, the matter will be reported to the appropriate authorities as soon as practical.

4.2. Data protection principles

4.2.1. All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR and the Data Protection Act 2018. KCLMS's policies and procedures are designed to ensure compliance with these principles.

4.2.2. Personal data must be processed lawfully, fairly and transparently

4.2.2.1. KCLMS will identify an applicable lawful basis prior to commencing any processing of personal data. It will ensure that it provides privacy notices written in accessible, plain language and which make available to data subjects the information to which they are entitled. This applies whether the personal data is to be obtained directly from the data subjects or from other sources.

4.2.2.2. As a minimum, privacy notices will include:

1. the identity (if not implied by context) and the contact details of the school
2. the contact details of the Data Protection Officer
3. the purposes of the processing for which the personal data is intended
4. the legal basis for the processing
5. the period for which the personal data will be retained
6. the existence of the rights of access, rectification, erasure and to object to processing
7. the conditions relating to exercising these rights
8. the categories of personal data concerned
9. where applicable, the recipients or categories of recipients of the personal data

10. where applicable, that the school intends to transfer personal data to a recipient in another country and the level of protection afforded to the data
11. any further information necessary to guarantee fair processing

4.2.3. Personal data must be collected for specific, explicit and legitimate purposes and not further processed

4.2.3.1. All datasets and processes will be recorded on the information asset register maintained by the Business Manager.

4.2.3.2. Data obtained for specified purposes must be used only for the purposes stated at the time of collection unless a further legal basis exists and is documented.

4.2.4. Personal data must be adequate, relevant and limited to what is necessary for processing

4.2.4.1. Collect and process personal data only to the extent that it is necessary for the operation and promotion of the school and in the best interests of the data subjects.

4.2.4.2. All data collection forms (electronic or paper-based) must include a privacy notice or link to a privacy statement and be approved by the Data Protection Officer.

4.2.4.3. The school will ensure that the effectiveness of its data protection and information security controls is subject to regular review within the internal audit programme.

4.2.5. Personal data must be accurate and kept up to date with every effort to erase or rectify without delay, when necessary

4.2.5.1. Data stored by KCLMS must be reviewed and updated as necessary. No data should be retained unless it is reasonable to assume that it is accurate.

4.2.5.2. Staff involved in the collection and processing of data must do so with due regard for accuracy.

4.2.5.3. Data subjects, including parents, students, staff and governors, carry an obligation to ensure that their data, held by KCLMS, is accurate and up to date. Application, enrolment and other collection forms must include a declaration by the subject that the data contained therein is accurate at the date of submission.

4.2.5.4. Data subjects must be informed of the need to notify KCLMS of any changes in circumstance in order that personal records can be updated accordingly. It is the responsibility of KCLMS to ensure that any notification regarding change of circumstances is recorded and acted upon in a timely manner.

4.2.5.5. The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the frequency with which it might change and any other relevant factors.

4.2.5.6. On at least an annual basis, the administrators of each dataset must review the retention status of the personal data for which they are responsible. This review will be undertaken in consultation with the Senior Leadership Team. Data that is no longer required in the context of the registered purpose must be securely terminated or anonymised.

4.2.5.7. The Data Protection Officer is responsible for managing requests for rectification from data subjects within 30 calendar days. If the school is unable to comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the Information Commissioner and seek judicial remedy.

4.2.5.8. Where third-party organisations may have been passed inaccurate or out-of-date personal data, the Data Protection Officer will make appropriate arrangements to inform the recipients that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned. Errors should be corrected where appropriate.

4.2.5.9. Personal data will be retained in line with the School's Data Retention Schedule and, once its retention period is achieved, it must be securely destroyed or anonymised.

4.2.5.10. Where personal data is retained beyond the processing date, it will be anonymised in order to protect the identity of the data subjects.

4.2.5.11. Any retention of data beyond the periods defined in the Data Retention Schedule must be authorised by the Data Protection Officer who will ensure that the justification is clearly identified and recorded in line with the requirements of data protection legislation.

4.2.6. Personal data must be processed in a manner that ensures appropriate security

4.2.6.1. The Data Protection Officer will advise the Business Manager on matters of information risk and mitigation measures both technical and organisational.

4.2.6.2. Technical security standards will be informed by the Information Security policy and agreed by the Finance and General Purposes Committee, which the Head Teacher and Business Manager attend.

4.2.6.3. Organisational measure will include:

1. Appropriate training for all KCLMS employees
2. Pre-employment checks
3. The inclusion of data protection in employment contracts
4. Inclusion of data protection obligations in the staff code of conduct
5. Robust disciplinary processes
6. Monitoring of security policy compliance
7. Physical access controls to electronic and paper-based records
8. The locking, when unoccupied, of any area in which personal data is present e.g. locking PC's when leaving workstation
9. The design and inception of new processes within the school
10. Secure storage of paper-based data
11. Restriction on the use of portable electronic devices including storage devices
12. Restrictions on the use of employee-owned personal devices to access school data
13. Protocols governing the control of personal data accessed remotely for the purposes of home working, visits etc.

4.2.7. KCLMS must be able to demonstrate accountability

4.2.7.1. KCLMS will demonstrate compliance with the data protection principles by requiring adherence to policies, codes of conduct and stated procedure. It will adopt techniques such as data protection by design and conduct Data Protection Impact Assessments according to agreed protocols.

4.2.7.2. In the event of a data breach, the school will invoke its data breach protocol and associated notification procedures where appropriate to do so.

4.3. Data subjects' rights

4.3.1. KCLMS will make provision such that data subjects can exercise:

1. Their right to be informed
2. Their right of access
3. Their right to rectification
4. Their right to erase
5. Their right to restrict processing
6. Their right to data portability
7. Their right to object
8. Their rights in relation to automated decision making and profiling

4.3.2. The standard Subject Access Request Procedure, provided by the ICO, sets down the means by which such requests will be discharged in compliance with the legislation.

4.3.3. Subject Access Requests should be made by submitting a Subject Access Request Form, which is available on the school's website (in the policies folder).

4.3.4. Data subjects have the right to complain to KCLMS in respect of the processing of their personal data. In such circumstances the handling of a request from a data subject will be subject to the terms of the school's Complaints Procedure.

4.4. Consent

4.4.1. Consent must be explicitly and freely given. It must be a specific, an informed and unambiguous indication of the data subject's agreement to the processing of their personal data. Consent must be signified by a statement or by a clear affirmative action. The data subject can withdraw their consent at any time.

4.4.2. Where the data subject is not considered competent to provide informed consent, processing must be authorised by the subject's next of kin as named on school systems.

4.4.3. Where special categories of data are to be processed, explicit written consent from the data subject must be obtained unless an alternative legal basis for processing exists.

4.4.4. Consent to process sensitive personal data must be obtained by using approved consent documents.

4.4.5. Where consent is the legal basis for processing, the process must be subject to an appropriate mechanism for managing that consent.

4.4.6. In the event where KCLMS provides online services to a child under 13 years of age, prior authorisation must be obtained from a person with parental responsibility.

4.5. Security of data

4.5.1. All employees including casual workers, volunteers, contractors and governors of KCLMS are responsible for the security of the data to which they have access. Policies, procedures and codes of practice determine the means by which information is secured.

4.5.2. Employees must adhere to specific protocols which protect against the inappropriate sharing of personal data with third parties.

4.5.3. Employees must not access school information systems or records for any purpose which is not directly required for the discharge of their contracted duties on behalf of the school.

4.5.4. Systems will be designed such that personal data is accessible only to those who have professional need of it and access must only be granted in line with authorised procedures.

4.5.5. KCLMS has a service level agreement with KCL to supply IT services. The security of data is covered by the KCL Information Security Policy. Detailed explanation of security measures can be found in this policy.

4.5.6. Manual records must not be left unattended where they could be accessed by unauthorised personnel. Manual records must not be removed from school premises without explicit authorisation. Manual records no longer required for day-to-day operation must be removed to secure archive storage.

4.5.7. Personal data may only be deleted or disposed of in line with the Data Retention Schedule. Manual records that have reached their retention date must be disposed of as 'confidential waste'. Removable media carrying or potentially carrying personal data should be referred to the KCL ICT Helpdesk for secure termination.

4.6. Disclosure of data

4.6.1. KCLMS must ensure that personal data is not disclosed to third parties, including family members and public bodies, without appropriate authority. All employees should exercise caution when asked to disclose personal data to anyone other than the confirmed data subject. Employees will receive scenario-based training to support their handling of such requests.

4.6.2. From time to time the school is required to share personal information with government and other agencies. Wherever possible, the school will make this clear in the Privacy Notices displayed at the point of collection.

4.6.3. The school will ensure that data passed to such recipients is complete, accurate and up to date. It will transfer only information to which the recipient has a statutory right, where legislation requires it or the subject has consented to the transfer. The school will take steps to ensure the security of such data up to the point where control passes to the recipient. Thereafter, handling of the shared information by the recipient will be subject to the terms of the recipient's privacy notices.

4.6.4. In most cases, data sharing with third parties will be handled by trained employees in a small number of roles. All requests to provide data to third parties must be documented and authorised by the Business Manager, and will be audited by the Data Protection Officer.

4.7. Retention and disposal of data

4.7.1. KCLMS will not keep personal data in a form that permits identification of data subjects for longer than the period necessary for the purpose(s) for which the data was originally collected.

4.7.2. The retention period for each category of personal data will be set out in the Information Asset Register. The Register will include the criteria used to determine such periods and state any statutory obligations to retain or erase data.

4.7.3. The Business Manager will maintain the Data Retention Periods, via the Information Asset Register, on behalf of the school.

4.7.4. KCLMS may store personal data for longer periods if it is to be processed solely for statistical research and archiving purposes which are in the public interest. In such circumstances, the school will implement technical and organisational measures to safeguard the rights and freedoms of data subjects.

4.7.5. Personal data, in all formats, must be disposed of in accordance with KCLMS secure disposal procedure.

4.8. Data transfers

4.8.1. KCLMS will only transfer personal data outside the EEA if one or more of the following safeguards, or exceptions, exist:

1. An adequacy decision
2. Privacy Shield assurance
3. Binding corporate rules
4. Model contract clauses

4.8.2. In the absence of any of the above, transfer of personal data to a third country or international organisation shall not take place unless at least one of the following conditions exists:

4.8.2.1. the data subject has explicitly consented to the proposed transfer having been informed of the possible risks of such transfers in the absence of appropriate safeguards.

4.8.2.2. the transfer is necessary for the performance of a contract between the data subject and the college or the implementation of pre-contractual measures taken at the data subject's request.

4.8.2.3. the transfer is necessary for the conclusion or performance of a contract between the college and another natural or legal person which is in the interest of the data subject.

4.8.2.4. the transfer is necessary for important reasons of public interest.

4.8.2.5. the transfer is necessary for the defence or exercising of legal claims by the school.

4.8.2.6. the transfer is necessary in order to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent.

4.9. Register of datasets and processes

4.9.1. KCLMS has established a register of datasets and processes, the information asset register, which defines:

1. business processes that use personal data
2. sources of personal data
3. classes of personal data involved
4. classes of data subject involved
5. purpose of the processing
6. recipients, and potential recipients, of the personal data
7. the system, repository or nature of the storage media
8. the data retention period

4.9.2. A Schedule of Retention Periods and disposal requirements is kept as part of the school's information asset register.

4.10. Risk and impact assessments

4.10.1. Prior to processing personal data, KCLMS will assess the level of risk to the rights and freedoms of data subjects. It will implement mitigation measures proportionate to the identified risk.

4.10.2. Where a new process is likely to result in a high risk, through the introduction of new technologies or due to its nature, scope or purpose, KCLMS shall, prior to the processing, carry out a Data Protection Impact Assessment (DPIA).

4.10.3. When required, DPIAs will be carried out in relation to the processing of personal data by KCLMS and processing undertaken by other organisations on its behalf.

4.10.4. Where a DPIA indicates that a planned process could cause damage and/or distress to the data subjects, the decision as to whether or not to proceed must be escalated for review to the Head Teacher via the DPO.

4.10.5. In the event that significant concerns exist regarding the potential for damage or distress, or in respect of the volume of data concerned, the DPO will advise the Head Teacher on the need to escalate the matter to the Information Commissioner.

4.10.6. In all cases, proportionate controls must be applied such that processing meets the requirements of the current legislation within the limits of risk exposure acceptable to the school.

4.11. External Data Processors and Cloud Computing

4.11.1. Authority to use external suppliers or partners to process personal information must be obtained from the Finance and General Purposes Committee. This applies to the use of

processing services to meet specific requirements; for example using external mailing houses or bureau services.

4.11.2. Prior to any data sharing or processing taking place, a Data Processor Agreement must be in force. The terms of such agreements must be proportionate to the potential for impact on the rights and freedoms of the data subjects.

4.11.3. The performance of the data processor must be sponsored by, and subject to the oversight of, a named responsible staff member and, from time to time, the DPO.

4.11.4. Proposals to use externally hosted (cloud) processing and/or data storage, as part of a school business system, must be referred to the Finance and General Purposes Committee and KCL IT service in order for security arrangements to be validated prior to entering any contract or the transfer of personal data.

4.11.5. The Finance and General Purposes Committee may, from time to time, delegate authorisation to the DPO, Business Manager or the Head Teacher.

4.12. Partnership working

4.12.1. Where the processing of personal data is carried out to support partnership activities between the school and other organisations, there must be a written data sharing agreement which includes a definition of the legal status of each partner in respect of Data Protection.

4.12.2. Parties should be designated as Data Controller, Data Controllers in Common, Joint Data Controllers or Data Processors. Advice should be sought from the DPO in determining these arrangements for particular initiatives.

4.13. Customer Service

4.13.1. Excellent Customer Service is expected in all aspects of school operation. Data Protection legislation should not be used as a reason to refuse to assist an enquirer or to prevent the progress of legitimate business.

4.13.2. While information security is paramount, there are, in almost all circumstances, correct ways to proceed which will be both compliant and helpful to individuals and the college.

4.13.3. Wherever possible (MIS student information screens for example) the school will provide contextual advice on how to respond to particular circumstances. However, if faced with a new or unexpected data protection question or situation, anyone concerned should contact the Data Protection Officer.

5. Implementation

5.1. The School aims to use personal data in the best interests of data subjects.

5.2. All employees, and others having access to data on behalf of the school, are required to use the policy mechanisms set out above and in associated documents to ensure legal compliance and the protection of personal information. Training and further support is available from the Business

Manager, the DPO and information listed on King's College London's Data Protection portal page.

5.3. In order to support the implementation of the above policy, the school will:

5.3.1. Appoint a named individual with specific responsibility for data protection in the organisation (the Data Protection Officer).

5.3.2. Ensure that the Finance and General Purposes Committee receives reports on Data Protection matters at its regular meetings.

5.3.3. Provide appropriate guidance materials and audited training for employees according to their role in handling personal information.

5.3.4. Ensure that employees understand that they have a contractual obligation to manage the personal data in their care appropriately.

5.3.5. Ensure that any third-party organisation that processes data on the school's behalf has adequate control measures in place and is subject to an appropriate contractual agreement.

5.3.6. Put in place appropriate systems to collect, store, manage, process and dispose of data and explain to employees that the use of alternative mechanisms is contrary to school policy.

5.3.7. Fully document systems, processes and data flows.

5.3.8. Ensure that security is a priority objective in the design of new systems and processes.

5.3.9. Conduct Data Privacy Impact Assessments prior to introducing new processes which are assessed as high-risk.

5.3.10. Ensure the robustness and security of physical and electronic systems for processing data and subject them to regular third-party review.

5.3.11. Ensure that detailed Privacy Notices, written in accessible language, are available to data subjects at the point of data collection and that these are regularly reviewed.

5.3.12. Ensure that data is not processed for purposes other than those stated unless some other over-riding lawful basis applies.

5.3.13. Establish internal mechanisms to manage formal requests for access to personal data from data subjects and third parties.

5.3.14. Establish internal mechanisms to manage potential, suspected and actual data-loss incidents.

5.3.15. Establish quality assurance mechanisms to ensure the integrity of data particularly in respect of high-volume processes.

6. Associated Documentation

6.1. The policy should be used in conjunction with the following associated documents:

- Fair Processing Notices
- Staff Code of Conduct
- Schedule of Data Retention Periods as detailed in the Information Asset Report
- ICT Acceptable Use Policy (Staff)
- s29 Protocol (disclosure of information to the Police and other law enforcement agencies)
- Subject Access Request Form
- Privacy Notices (Students, Parents/Carers)
- Privacy Notices (Staff)

5.2 Associated Legislation:

- Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Privacy of Electronic Communications Regulations 2003

7. Monitoring, Review and Evaluation

7.1. The Data Protection Officer and associated link governor are both responsible for the maintenance, review and monitoring of the Data Protection Policy.

7.2. The policy, and any subsequent versions of it, will be formally adopted on behalf of the school, subject to the recommendation of the Finance and General Purposes Committee, and formal approval by the Full Governing Board.

7.3. This policy will be subject to regular informal monitoring and review by the DPO and associated link governor.

7.4. This policy will be formally reviewed by the Finance and General Purposes Committee at intervals of not less than 2 years.

7.5. Copies of this policy and associated documents are available from the school's website and portal.