LANCASTER UNIVERSITY
SCHOOL OF MATHEMATICS

# Lancaster University School of Mathematics

## Data Protection Policy

Lancaster University

RIGBY EDUCATION TRUST

CARDINAL NEWMAN COLLEGE

| Title | Data Protection Policy |
|---|---|
| **Approved** | December 2024 |
| **Review Date** | December 2027 |

The Rigby Education Maths School was set-up to operate and oversee the Lancaster University School of Mathematics.

The Rigby Education Maths School is an academy trust and a charity. The Lancaster University School of Mathematics is the charitable activity of the academy trust. Therefore, in this document references to the Maths School apply to the Rigby Education Maths School.

## Contents

# 1.0. Introduction

## 1.1. Purpose

The Lancaster University School of Mathematics collects and processes personal information belonging to applicants, students, employees, governors, contractors and others in line with the data protection Act 2018. This is the UK's implementation of the General Data Protection Regulation 2016.

Section 1.2 below details some key definitions used within this policy.

## 1.2. Definitions

**Material scope** – data protection legislation applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

**Territorial scope** – data protection legislation applies to data controllers who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the UK that process personal data in order to offer goods and services or monitor the behaviour of data subjects who are resident in the UK.

**Personal data** – any information relating to an identified or identifiable natural person ('data subject').

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.

**Special categories of personal data** – 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.

**Data controller** – 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.

**Data subject** – any living individual who is the subject of personal data held by an organisation.

**Processing** – 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.

**Profiling** – is 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. 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.

**Personal data breach** – 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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

**Data subject consent** - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

**Child** – 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

**Third party** – 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.

**Filing system** – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

## 2.0. Policy statement

The Board of Trustees is committed to compliance with all relevant laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information the Maths School collects and processes in accordance with data protection legislation.

Compliance with the data protection legislationis described by this policy and other relevant policies along with connected processes and procedures.

Data protection legislation and this policy apply to all the Maths School's personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the organisation processes from any source.

The Data Protection Officer (DPO) is responsible for reviewing the Maths School register of processing annually in the light of any changes to the Maths School's activities (as determined by changes to the data register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.

This policy applies to all employees and contractors. Any breach will be dealt with under the Maths School's policies and may also be a criminal offence.

Partners and any third parties working with or for the Maths School, 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 personal data held by the Maths School without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which the Maths School is committed, and which gives the Maths School the right to audit compliance with the agreement.

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.

## 3.0. Responsibilities and roles under the General Data Protection Regulation

The Maths School is a data controller and data processor under data protection legislation.

The Senior Leadership Team and all those in managerial or supervisory roles throughout the Maths School are responsible for developing and encouraging good information handling practices within the Maths School; responsibilities are set out in individual job descriptions.

The Data Protection Officer (DPO) should be a suitably qualified and experienced member ofstaff. They will be accountable for the management of personal data within the Maths School and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

- development and implementation of the GDPR as required by this policy; and
- security and risk management in relation to compliance with the policy.

The DPO has been appointed to take responsibility for the Maths School's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the Maths School complies with the GDPR, as do managers in respect of data processing that takes place within their area of responsibility.

The DPO has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for employees seeking clarification on any aspect of data protection compliance.

Compliance with data protection legislation is the responsibility of all employees of the Maths School who process personal data.

Employees and contractors of the Maths School are responsible for ensuring that any personal data about them and supplied by them to the Maths School is accurate and up to date.

## 4.0. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in data protection legislation. The Maths School's policies and procedures are designed to ensure compliance with the principles.

**Personal data must be processed lawfully, fairly and transparently**

**Lawful** – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

**Fairly** – in order for processing to be fair, the data controller must make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

**Transparently** – data protection legislation includes rules on giving privacy information to data subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language. This must include:

- the identity and the contact details of the controller and, if any, of the controller's representative
- the contact details of the Data Protection Officer
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- the period for which the personal data will be stored
- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected
- the categories of personal data concerned
- the recipients or categories of recipients of the personal data, where applicable
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data
- any further information necessary to guarantee fair processing.

**Personal data can only be collected for specific, explicit and legitimate purposes and not further processed**

All datasets and processes will be recorded on the data asset register maintained by the DPO.

Data obtained for specified purposes must not be used for a purpose that differs from the use stated unless a further legal basis exists and is documented.

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

The DPO is responsible for ensuring that the Maths School does not collect information that is not strictly necessary for the purpose for which it is obtained.

All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the DPO.

The DPO will ensure that, on an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.

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

Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

The DPO is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

It is also the responsibility of the data subject to ensure that data held by the Maths School is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

Employees, students and others should be required to notify the Maths School of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Maths School to ensure that any notification regarding change of circumstances is recorded and acted upon.

The DPO 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 speed with which it might change and any other relevant factors.

On at least an annual basis, the DPO will review the retention dates of all the personal data processed by the Maths School, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed.

The DPO is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If the Maths School decides not to comply with the request, the DPO must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

The DPO is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

Where personal data is retained beyond the processing date, it will be retained in a format designed to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

The DPO must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

**Personal data must be processed in a manner that ensures the appropriate security**

The DPO will carry out a risk assessment considering all the circumstances of the Maths School's controlling or processing operations.

In determining appropriateness, the DPO should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or students) if a security breach occurs, the effect of any security breach on the Maths School itself, and any likely reputational damage.

When assessing appropriate technical measures, the DPO will consider the following:

- Password protection.
- Automatic locking of idle terminals.
- Removal of access rights for USB and other memory media.
- Virus checking software and firewalls.
- Role-based access rights including those assigned to temporary staff.

- Encryption of devices that leave the organisations premises such as laptops.
- Security of local and wide area networks.
- Privacy enhancing technologies such as pseudonymisation and anonymisation
- Identifying appropriate international security standards relevant to the Maths School.

When assessing appropriate organisational measures, the DPO will consider the following:

- The appropriate training levels throughout the Maths School.
- Measures that consider the reliability of employees (such as references etc.).
- The inclusion of data protection in employment contracts.
- Identification of disciplinary action measures for data breaches.
- Monitoring of staff for compliance with relevant security standards.
- Physical access controls to electronic and paper-based records.
- Adoption of a clear desk policy.
- Storing of paper-based data in lockable fire-proof cabinets.
- Restricting the use of portable electronic devices outside of the workplace.
- Restricting the use of employee's own personal devices being used in the workplace.
- Adopting clear rules about passwords.
- Making regular backups of personal data and storing the media off-site.
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the European Economic Area.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

**The Maths School must be able to demonstrate accountability.**

The Maths School will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

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

## 5.0. Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them. Rights to:

- Make subject access requests regarding the nature of information held and to whom it has been disclosed.
- Prevent processing likely to cause damage or distress.
- Prevent processing for purposes of direct marketing.
- Be informed about the mechanics of automated decision-taking process that will significantly affect them.
- Not have significant decisions that will affect them taken solely by automated process.
- Sue for compensation if they suffer damage by any contravention of the GDPR.
- Take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
- Request the supervisory authority to assess whether any provision of the GDPR has been contravened.
- Have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- Object to any automated profiling that is occurring without consent.

The Maths School ensures that data subjects may exercise these rights:

- Data subjects may make data access requests as described in Subject Access Request Procedure; this procedure also describes how the Maths School will ensure that its response to the data access request complies with the requirements of the GDPR.
- Data subjects have the right to complain to the Maths School relating to the processing of their personal data, the handling of a request, and appeal on how complaints have been handled in line with the Complaints Procedure.

## 6.0. Consent

The Maths School understands 'consent' to mean that it has been explicitly and freely given, any specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

The Maths School understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.

For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances, consent to process personal and sensitive data is obtained routinely by the Maths School using standard consent documents e.g. when a student enrols.

## 7.0. Security of data

All employees are responsible for ensuring that any personal data that the Maths School holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the Maths School to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Procedure. All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access when during working hours
- in a locked drawer or filing cabinet out-of-hours
- if computerised, password protected in line with corporate requirements in the Access Control Procedure
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised employees of the Maths School. All employees are required to enter into an Acceptable Use Policy before they are given access to organisational information of any sort, which details rules on screen time-outs.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit [written] authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving.

Personal data may only be deleted or disposed of in line with the Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

## 8.0. Disclosure of data

The Maths School must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All employees should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Maths School's business.

The GDPR permits certain disclosures without consent including:

- prevention or detection of crime including the apprehension or prosecution of offenders
- prevention of serious harm to a third party
- protection the vital interests of the individual.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO.

## 9.0. Retention and disposal of data

The Maths School shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

The Maths School may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations the Maths School has to retain the data.

The Maths School's data retention and data disposal procedures will apply in all cases.

Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

## 10.0. Data transfers

Exports of data to the European Economic Area (EEA) is permitted. Exports of data to other countries are subject to specific arrangements based on adequacy rules reflecting the level of protection for the fundamental rights of the data subjects.

Binding corporate rules- the Maths School may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that the Maths School is seeking to rely upon.

Model contract clauses - the Maths School may adopt approved model contract clauses for the transfer of data outside of the EEA. If the Maths School adopts model contract clauses approved by the relevant supervisory authority] there is an automatic recognition of adequacy.

The advice of the DPO will be sought in relation to all data transfers to countries outside the EEA.

## 11.0. Information asset register/data inventory

The Maths School will develop a data inventory as part of its approach to address risks and opportunities:

- business processes that use personal data
- source of personal data
- volume of data subjects
- description of each item of personal data
- processing activity
- maintains the inventory of data categories of personal data processed
- documents the purpose(s) for which each category of personal data is used
- recipients, and potential recipients, of the personal data
- the role of the Maths School throughout the data flow
- key systems and repositories
- any data transfers
- all retention and disposal requirements.

The Maths School is aware of any risks associated with the processing of particular types of personal data.

The Maths School assesses the level of risk to individuals associated with the processing of their personal data.

The Maths School shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, the Maths School shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

Where, as a result of a DPIA it is clear that the Maths School is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not the Maths School may proceed must be escalated for review to the DPO.

The DPO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

## 12.0. External Data Processors and Cloud Computing

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.

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.

Where the processing of personal data is carried out to support partnership activities between the Maths 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.

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 any specific initiatives.

## 13.0. Customer Service

Excellent Customer Service is expected in all aspects of Maths 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.

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 trust.

Wherever possible the Maths School will provide contextual advice on how to respond to specific circumstances. However, if faced with a new or unexpected data protection question or situation, anyone concerned should contact the DPO.

## 14.0. Implementation

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

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

In order to support the implementation of the above policy, the Maths School will:

- Appoint a named individual with specific responsibility for data protection in the organisation (the Data Protection Officer).
- Ensure that the Finance, Audit and Risk Committee is briefed and updated on data protection.
- Provide appropriate guidance materials and audited training for employees according to their role in handling personal information.
- Ensure that employees understand that they have a contractual obligation to manage the personal data in their care appropriately.
- Ensure that any third-party organisation that processes data on the Maths School's behalf has adequate control measures in place and is subject to an appropriate contractual agreement.
- 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 Maths School policy.
- Fully document systems, processes and data flows.
- Ensure that security is a priority objective in the design of new systems and processes.
- Conduct Data Privacy Impact Assessments prior to introducing new processes which are assessed as high-risk.
- Ensure the robustness and security of physical and electronic systems for processing data and subject them to regular third-party review.
- 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.
- Ensure that data is not processed for purposes other than those stated unless some other over-riding lawful basis applies.

- Establish internal mechanisms to manage formal requests for access to personal data from data subjects and third parties.
- Establish internal mechanisms to manage potential, suspected and actual data-loss incidents.
- Establish quality assurance mechanisms to ensure the integrity of data particularly in respect of high-volume processes.

## 15.0. Monitoring, Review and Evaluation

The DPO is responsible for the maintenance, review and monitoring of the Data Protection Policy.

The policy, and any subsequent versions of it, will be formally adopted on behalf of the Maths School, subject to the recommendation of the Finance, Audit and Risk Committee, and formal approval by the Board of Trustees.

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

Copies of this policy and associated documents are available from the Maths School's website.

## 16.0. Review cycle

This policy statement will be reviewed at least every three years.