EXETER MATHS SCHOOL

FREEDOM FOR THINKERS

Data Protection Policy

Staff reviewer:	Scrutinised by link Governor:	Date signed off at Committee:	Date approved at Board:	Next review date:
Nicola Mitchell	Jenny Leach	8th June 2021	NA	May 2023

Table of Contents

1. Purpose

1.1. Exeter Mathematics School collects and processes personal information belonging to applicants, students, employees, governors, contractors and others in line with the Data Protections Act 2018.

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. Definitions

2.1. 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.

2.2. 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.

2.3. Data Protection Officer (DPO)

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.

The Data Protection Officer role will be designated to the School Business Manager in the first instance. However, in their absence and the request is urgent, the Headteacher and/or Deputy Headteacher will assume the role.

2.4. Data Subject

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

2.5. Explicit consent

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

2.6. Filing system

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

2.7. General Data Protection Regulation (GDPR)

The GDPR is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union. Adopted in April 2016, the regulation came into full effect in May 2018. The GDPR is enshrined in UK law by the Data Protection Act 2018.

2.8. Legal person

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

2.9. Natural person

An individual human being, with consciousness of self

2.10. Personal data

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

Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Identifiers are for example: name, contact details, identification number, location data, online identifier, photographs, video recordings, communications, medical data (including occupational health), behaviour data, performance related information, financial data, genetic information, cultural or social information.

2.11. 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.

2.12. 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.

2.13. Profiling

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.

2.14. 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, data concerning health or data concerning an individual's sex life or sexual orientation.

2.15. 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.

3. Policy

3.1. Overview

Exeter Mathematics School 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 Policy and its associated documents and procedures.

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.

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

Partners and any third parties working with or for Exeter Mathematics 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 or receive personal data controlled by Exeter Mathematics School without having first entered into a data sharing 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.

3.2. Data protection principles

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. Exeter Mathematics School's policies and procedures are designed to ensure compliance with these principles.

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

Exeter Mathematics School 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.

Personal data must 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 be used only for the purposes stated at the time of collection unless a further legal basis exists and is documented.

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

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

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.

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.

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

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

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

Data subjects, including parents, students, staff and governors, carry an obligation to ensure that their data, held by Exeter Mathematics School, 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.

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

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 destroyed or anonymised.

The Data Protection Officer is responsible for managing requests for rectification from data subjects within one month. 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.

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.

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.

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

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.

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

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

Technical security standards will be informed by the Information Security policy and agreed by the Finance and Resources Committee of which the Headteacher and DPO are each members.

Organisational measure will include:

- Appropriate training for all Exeter Mathematics School employees
- Pre-employment checks
- The inclusion of data protection in employment contracts
- Inclusion of data protection obligations in the staff code of conduct
- Robust disciplinary processes

- Monitoring of security policy compliance
- Physical access controls to electronic and paper based records
- The locking, when unoccupied, of any area in which personal data is present e.g. locking PCs when leaving workstation
- Adoption of a clear desk policy
- The design and inception of new processes within the school
- Secure storage of paper-based data
- Restriction on the use of portable electronic devices including storage devices
- Restrictions on the use of employee-owned personal devices to access school data
- Protocols governing the control of personal data accessed remotely for the purposes of home working, visits etc.

3.4. Exeter Mathematics School must be able to demonstrate accountability

Exeter Mathematics School 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.

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

3.5. Data subjects' rights

Exeter Mathematics School will make provision such that data subjects can exercise:

- Their right to be informed
- Their right of access
- Their right to rectification
- Their right to erase
- Their right to restrict processing
- Their right to data portability
- Their right to object
- Their rights in relation to automated decision making and profiling

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.

Data subjects have the right to complain to Exeter Mathematics School 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.

3.6. Consent

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.

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.

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.

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

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

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

3.7. Security of data

All employees including casual workers, volunteers, contractors and governors of Exeter Mathematics School 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.

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

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.

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.

Exeter Mathematics School has a service level agreement with Exeter College to supply IT services. The security of data is covered by the Exeter College Information Security Policy. Detailed explanation of security measures can be found in the associated Information Security policy.

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.

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 Exeter College ICT Helpdesk for secure termination.

3.8. Disclosure of data

Exeter Mathematics School 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.

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.

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.

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 Data Protection Officer.

3.9. Retention and disposal of data

Exeter Mathematics School 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.

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

The Data Protection Officer will maintain the Data Retention Periods, via the Data Asset Register, on behalf of the school.

Exeter Mathematics School 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.

Personal data, in all formats, must be disposed of in accordance with Exeter College's secure disposal procedure.

3.10. Data transfers

Exeter Mathematics School will only transfer personal data outside the EEA if one or more of the following safeguards, or exceptions, exist:

- An adequacy decision
- Privacy Shield assurance
- Binding corporate rules
- Model contract clauses

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:

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.

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.

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.

the transfer is necessary for important reasons of public interest.

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

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.

3.11. Register of datasets and processes

Exeter Mathematics School has established a register of datasets and processes which defines:

- business processes that use personal data
- sources of personal data
- volume of data subjects
- classes of personal data involved
- classes of data subject involved
- purpose of the processing
- recipients, and potential recipients, of the personal data
- the system, repository or nature of the storage media

The Data Protection Officer maintains a description of the flow of data between processes within school functions.

The Data Protection Officer maintains a Schedule of Retention Periods and disposal requirements.

3.12. Risk and impact assessments

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

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

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

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 Headteacher via the DPO

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 Headteacher on the need to escalate the matter to the Information Commissioner.

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.

3.13. External Data Processors and Cloud Computing

Authority to use external suppliers or partners to process personal information must be obtained from the Resource Committee. This applies to the use of processing services to meet specific requirements; for example, using external mailing houses or bureau services.

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.

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

The Resources Committee may, from time to time, delegate authorisation to the DPO or the Headteacher.

3.14. Partnership working

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.

Parties should be designated as Data Controller, Joint Data Controllers or Data Processors. Advice should be sought from the Data Protection Officer in determining these arrangements for any specific initiatives.

3.15. Customer Service

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.

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.

Wherever possible (MIS student information screens for example) the 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 Data Protection Officer.

4. Implementation

The 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 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 DPO and information listed on the Data Protection portal page.

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

- Appoint a named individual with specific responsibility for data protection in the organisation (the Data Protection Officer).
- Ensure that the Resources Committee receives reports on Data Protection matters at its regular meetings.
- 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 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 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.

5. Associated Documentation

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

- Data Asset Register
- Data Breach Protocol
- Data Impact Assessment
- Fair Processing Notices including:
- Privacy Notice – Staff
- Privacy Notice – Students
- Privacy Notice - Governors
- ICO Certificate
- Code of Practice for the collection, storage and use of students' personal information
- Schedule of Data Retention Periods
- Accessing learners' personal information – guide for parents and guardians
- Department for Education (2018) Information Sharing advice for practitioners providing safeguarding services to Children, young people, parents, and carers
- Information Commissioner's Office (2011) Data sharing code of Practice Data available at: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf
- Subject access request procedure

- Relevant Exeter College Policies as providers of HR, ICT and Student support under a Service Level Agreement
- Code of Practice for Systems Administrators – Exeter College who provide ICT Networks under SLA
- Information Security Policy – Exeter College policy under SLA

5.1. Associated Legislation:

- UK 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
- Annex C (disclosure of information to the Police and other law enforcement agencies)

6. Monitoring, Review and Evaluation

The Data Protection Officer and associated link governor are both 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 school, subject to the recommendation of the Resources Committee, and formal approval by the Full Governing Board.

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

This policy will be formally reviewed at intervals of no less than 2 years by the Resources Committee.

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

7. Equality Analysis

The following equality analysis section should be completed by the policy holder as part of every policy review and carries the same date as the main policy. EAs are particularly helpful in revealing any unintended, indirect discrimination.

Under the Equality Act (2010) we have a duty to

- Eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Act.
- Advance equality of opportunity between people who share a protected characteristic and those who do not.
- Foster good relations between people who share a protected characteristic and those who do not.

We need to consider each protected characteristic individually and in combination. The interaction of different layers of characteristics is called intersectionality. This recognises that the barriers for each group are not

homogenous, and instead are a combination of layers of identity interacting. For further detail or to support the completion of the following, please see our equality and diversity policy.

1. **Evidence considered** *What data or other information have you used to evaluate if this proposal is likely to have a positive or an adverse impact upon protected groups when implemented? Where were information gaps, and what steps can you take to remedy these gaps? Can the RM intelligence Dashboard (student counts) provide any insight into which protected characteristics are likely to be affected by the changes?*
   Exeter College Data Protection Policy reviewed last year
   Review of Associated Documentation to check it I still relevant

2. **Consultation.** *How have you consulted staff and student communities and representatives including those from protected groups? What were their views? Who else has been consulted in this proposal?*
   Consultation with Senior Leadership Team, and Link Governor

3. **Promoting equality.** *Does this policy have a positive impact on equality? What evidence is there to support this? Could it do more?*
   Y**es** - protecting the rights of individuals

4. **Identifying the impact of policies**

Identify any issues in the document which could have an adverse impact on any people who are protected by the Equality Act 2010. The protected characteristics are:

1. Age
2. Disability
3. Gender reassignment
4. Marriage and civil partnership
5. Pregnancy and maternity
6. Race
7. Religion or beliefs
8. Sex
9. Sexual orientation

None - although worth noting that gender reassignment, pregnancy and disability data are not classed as 'special category' they would have the same protections as data classed as 'personal'. It is possible their data could be treated as 'special category' data if this information can infer an individuals identity

Issue Assessed *E.g. policy section or practice.*	**Protected Group**	**Impact and Evidence** *What are the possible impacts on people from the protected groups above and explain how you have made that assessment. Are these impacts positive or negative?*	**Justification** *Can the issue be justified for academic or business reasons? Please explain.*	**Proposed Action/Timeline** *If this has a negative impact, what will you do to reduce, minimise, or eliminate negative impact? If this has a positive impact, how will you promote, develop, or utilise this opportunity?*	**Person responsible for action(s)**

5. **Monitoring** *How will you monitor the actual impact that your proposal has had following its implementation? When will you do this?*
   1. Data Breaches
   2. Data Protection Impact Assessments
   3. Training records

   All above shared and minuted at Resources Committee

6. **Summary** *Summarise the outcome of this Equality Assessment and state any actions you will be taking as a result.*
   This policy is equitable