



AXIOM MATHS DATA PROTECTION POLICY

Last review:	January 2024	Owner:	Data Protection Lead
Next review:	January 2025	Approval:	Board
Contact email:	info@axiommaths.com		

Contents

Introduction and Definitions.....	1
Data Protection Principles.....	2
1. Rights of Data Subject	2
2. Lawful, Fair and Transparent Data Processing	2
3. Personal Data Collected, Held and Processed.....	4
4. Accuracy of Data and Keeping Data Up to Date.....	5
5. Data Retention	6
6. Accounting and Record Keeping.....	6
7. Data Protection Impact Assessments	6
8. Keeping Data Subjects Informed	7
9. Subject Access Requests	8
10. Rectification of Personal Data.....	8
11. Erasure of Personal Data	8
12. Restriction of Personal Data Processing.....	9
13. Objections to Personal Data Processing.....	9
14. Other rights	10
15. Profiling and Automated Decision Making.....	10
16. Data Security.....	10
17. Organisational Measures	13
18. Transferring Personal Data to a Country Out of the EEA/ UK	14
19. Data Breach Notification.....	14
20. Implementation of Policy	15
21. Complaints.....	15
22. Contact – DPO information	15

INTRODUCTION AND DEFINITIONS

Note: we have recently changed our name from Mathematics Education for Social Mobility and Excellence (MESME) to Axiom Maths. During this transitionary period, some pages / documents / forms may refer to our old name. The way we process data and data subjects' rights are not changing so for the purposes of data protection, any referral to MESME or Axiom Maths are reference to the same organisation and are equally valid.

Introduction

This policy sets out Axiom Maths' (previously MESME) obligations regarding data protection and the rights of students, staff, teachers, mentors and those who use our services ("data subjects") under the UK GDPR as defined in section 3(10) (as supplemented by section 205(4)) of the DPA 2018 ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018" or referred to as "The Act").

This Policy documents Axiom Maths' obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out within this policy must be adhered to by Axiom Maths, its employees, contractors, or other parties working on our behalf.

This policy is intended to ensure that all personal information is handled properly, securely and in accordance with the UK General Data Protection Regulation (UK GDPR) and other legislation.

Definitions

The terms in this document have the meanings as set out in Article 4 and Article 9(1) of the GDPR unless amended by the Act.

For clarity, the following have been listed below:

'Personal Data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location, or online identities.

'Data Controller' means the legal or natural person, an agency, a public authority, or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by the Domestic Law, the controller (or the criteria for nominating the controller) may be designated by the law.

'Processing' means any operation or set of operations 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.

'Special Category Personal Data' means personal data that reveals racial or ethnic origin; political opinions; religious or philosophical beliefs, trade union membership, 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.

When Special Category Data is processed, it is given special protection, where additional safeguards are applied to collect and use this data.

Data relating to criminal convictions shall only be held and processed where there is legal authority and basis to do so.

DATA PROTECTION PRINCIPLES

Article 5 (1) and (2) sets out the key principles at the centre of the UK General Data Protection Regulation (GDPR) which any party handling personal data must comply. All personal data must be:

- Processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met.
- Collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes.
- Adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed.
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- Personal data processed shall not be kept in a form which permits identification of individuals for longer than is necessary for that purpose / those purposes.
- Processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
- Processed in such a way that demonstrates our accountability and responsibility with the UK GDPR and the Act.

1. RIGHTS OF DATA SUBJECT

The UK GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details:

- i. The right to be informed (Part 10):
- ii. The right of access (Part 11):
- iii. The right to rectification (Part 12):
- iv. The right to erasure (also known as the 'right to be forgotten') (Part 13):
- v. The right to restrict processing (Part 14):
- vi. The right to object (Part 15); and
- vii. The right to data portability (Part 16):
- viii. Rights with respect to automated decision-making and profiling (Part 17).

2. LAWFUL, FAIR AND TRANSPARENT DATA PROCESSING

The UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The UK GDPR

states that processing of personal data shall be lawful if at least one of the following applies:

- i. The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.
- ii. The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.
- iii. The processing is necessary for the performance of a legal obligation to which we are subject.
- iv. The processing is necessary to protect the vital interests of the individual or another.
- v. The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.
- vi. The processing is necessary for a legitimate interest of the charity or that of a third party, except where this interest is overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Special Categories of Personal Data

If the personal data being processed is “Special Category Data” (also known as “sensitive personal data”) processing is prohibited, unless one, or more, of the following exemptions applies:

- i. The data subject has given their explicit consent to process such data for the specified purposes (unless EU or UK law prohibits them from doing so).
- ii. The processing is necessary for the purpose of carrying out the controller’s obligations and exercising specific rights of the data controller or of the data subject in the field of employment and social protection law.
- iii. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- iv. The data controller is a charity or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in accordance with its legitimate activities, ensuring that the processing relates solely to its members or former members of that body or to persons who have regular contact with the body in relation to its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects.
- v. The processing relates to personal data which is made public by the data subject.
- vi. The processing is necessary for conducting legal claims or whenever courts are acting in their legal capacity.
- vii. The processing is necessary for substantial public interest, on the basis of domestic law which shall be proportionate to the aim of collection, shall respect the principles of data protection, and provide suitable and specific measures to safeguard the fundamental rights and interests of the data subject.
- viii. The processing is necessary for preventative or occupational medicine, for the assessment of an employee’s working capacity, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of domestic law or pursuant to a

contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR.

- ix. The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
- x. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Where special category personal data is processed the charity shall have both a lawful basis from Article 6 for using that personal data and at least one of the exemptions from Article 9(2) shall apply.

3. PERSONAL DATA COLLECTED, HELD AND PROCESSED

Axiom Maths processes personal data on beneficiaries, staff, clients and other individuals. In each case, the personal data must be processed in accordance with the data protection principles as outlined above.

Axiom Maths collects and processes the personal data set out in this part of the Policy. This includes:

- i. Personal data collected directly from data subjects and personal data obtained from third parties.
- ii. The charity only collects, processes, and holds personal data for the specific purposes set out in this part of the Policy (or for other purposes expressly permitted by the UK GDPR).
- iii. Data subjects are kept informed at all times of the purpose(s) the charity uses to process their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

Students

The personal data held about students may include name, contact details, parent/carer details, unique pupil number (UPN), date of birth, age, school details, school year, gender, ethnicity, Pupil Premium status, SEND status, attendance, progress and feedback on Axiom Maths programmes and academic attainment. This data will be collected and processed by Axiom Maths and organisations who are delivering programmes funded by Axiom Maths. The purpose of this data is to ensure the effective delivery of the programmes and to keep track of the number, attendance and demographics of beneficiaries.

This data will also be used to measure and track the short, medium and long-term impact of the Axiom Maths programmes. To track the long-term impact, data may be shared with an external research organisation to analyse the impact on student attainment compared to national statistics. As part of this research, the Department for

Education (DfE) may collect subsequent data, such as exam results and academic destinations, from national student databases. Subsequent data collected by the DfE will only be used to further analyse the impact of the programmes and will only be shared in anonymised format.

Employees

The personal data held about employees will include contact details, employment history, information relating to career progression, information relating to Disclosure and Barring Service (DBS) checks and photographs, as well as information required to administer their terms and conditions of employment.

This purpose of holding this data is to comply with legal obligations placed on Axiom Maths, as an educational charity, in relation to employment. Axiom Maths may pass information to other regulatory authorities where appropriate and may use names and photographs of staff in publicity and promotional material. Photographs of staff will not be shared without consent, and this will be requested from employees as and when needed.

Employees should note that information about disciplinary action may be kept for longer than the duration stated on the disciplinary policy. Although treated as “spent” once the stated time to be kept on record has expired, the details of the incident may need to be kept for a longer period.

Any wish to limit or object to the way Axiom Maths uses personal data should be communicated in writing to Axiom Maths’ Data Protection Lead. They will ensure that this objection is recorded and adhered to if judged to be appropriate by Axiom Maths Data Protection Lead, in consultation with Axiom Maths’ CEO. If the Axiom Maths Data Protection Lead is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why their request will not be granted.

Other Organisations/Individuals

Axiom Maths holds data about organisations/individuals to provide an effective service and fulfil the obligations as set out in our contracts. The level and detail of information held depends on the nature of the programme. Data is anonymised wherever possible and always held securely.

Axiom Maths may hold personal information in relation to other individuals who have contact with us, such as those submitting enquiries on our website, volunteers, and guests. Such information will be held only in accordance with the data protection principles and will not be kept longer than necessary to provide the service which it was collected for.

4. ACCURACY OF DATA AND KEEPING DATA UP TO DATE

Axiom Maths will take all reasonable steps to ensure that all personal data collected, processed, and held is kept accurate and up to date.

The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken to amend or erase that data without delay.

5. DATA RETENTION

Axiom Maths shall not keep personal data for any longer than is necessary for the purpose(s) for which that personal data was originally collected, held, and processed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise securely dispose of that data without delay.

For full details of Axiom Maths' approach to data retention, including retention periods for specific personal data types held by Axiom Maths please refer to Axiom Maths' Data Retention Policy.

6. ACCOUNTING AND RECORD KEEPING

The Data Protection Lead shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, Axiom Maths' other data protection-related policies, and with the UK GDPR and other applicable data protection legislation.

Axiom Maths shall keep written records of all personal data collections, where this is stored, and details of processing which shall incorporate the following information:

- i. The name and details of Axiom Maths, its Data Protection Lead, and any applicable third-party data processors.
- ii. The purposes for which the charity collects, holds, and processes personal data.
- iii. Details of the categories of personal data collected, held, and processed by the charity, and the categories of data subject to which that personal data relates.
- iv. Details of any transfers of personal data outside of the UK or European Economic Area (EEA) including details of how this data is shared and any safeguards to protect the data being shared.
- v. Details of how long personal data will be retained by the charity (please refer to Axiom Maths' Data Retention Policy); and
- vi. Detailed descriptions of all technical and organisational measures taken by the charity to ensure the security of personal data.

7. DATA PROTECTION IMPACT ASSESSMENTS

Axiom Maths will carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the UK GDPR and/or the processing involves the use of new or innovative technologies.

Data Protection Impact Assessments shall be overseen by the Data Protection Lead and shall address the following:

- i. Axiom Maths' objectives for the collection and processing of personal data
- ii. The type(s) of personal data that will be collected, held, and processed
- iii. Describe the nature, scope, context and purposes of the processing
- iv. Assess the necessity and proportionality of data processing
- v. The parties (internal and/or external) who will be consulted about the processing
- vi. The Risks posed to data subjects and to Axiom Maths
- vii. The proposed measures to minimise and mitigate the identified risks.

Axiom Maths shall provide reasonable assistance to individuals, schools or organisations (The Customer) wishing to 'access' maths circles with any Data Protection Impact Assessments or regulatory consultation that the Customer is legally required to make under Data Protection Laws in relation to the processing of that Customer's Personal Data.

8. KEEPING DATA SUBJECTS INFORMED

Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection. Where appropriate, parental consent will be sought; and

Where personal data is obtained from a third party, the relevant data subjects will be informed:

- i. Of the purpose of the collection or sharing of personal data:
- ii. if the personal data is used to communicate with the data subject, when the first communication is made; or
- iii. if the personal data is to be transferred to another party, before that transfer is made; or
- iv. as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

The following information shall be provided:

- i. Details of Axiom Maths including the identity of its Data Protection Lead:
- ii. The purpose(s) for which the personal data is being collected and processed (as detailed in Part 5 of this Policy) and the legal basis for the collection and processing of personal data:
- iii. Where applicable, the legitimate interests which the charity are using to justify collection and processing of personal data:
- iv. Where the personal data is not obtained directly from the data subject, the categories of personal data shared and processed:
- v. Where the personal data is transferred to one or more third parties, details of those parties:
- vi. Where the personal data is to be transferred to a third party that is located outside of the EEA, details of that transfer, including the appropriate safeguards in place to protect this data (see Part 13 of this Policy for further details):
- vii. How long the data will be processed and retained; including any anonymisation or long-term storage for statistical purposes:
- viii. The data subject's rights under the UK GDPR including the right to withdraw their consent to the processing of their personal data at any time:
- ix. Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the UK GDPR):
- x. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- xi. Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

9. SUBJECT ACCESS REQUESTS

Data subjects, employees and beneficiaries can make a Subject Access Request ("SARs") at any time to view the personal data which Axiom Maths holds about them, how that personal data is used, and why. They are encouraged to make these requests by emailing info@axiommaths.com.

Responses to SARs shall normally be made within one calendar month, however where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Responses to SARs shall be dependent upon the terms of the UK GDPR, the Data Protection Act (2018) and associated ICO guidance.

Axiom Maths does not charge a fee for the handling of normal SARs. We reserve the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

10. RECTIFICATION OF PERSONAL DATA

An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to Axiom Maths' Data Protection Lead, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified within one month. The period can be extended by up to two months in the case of complex requests. If additional time is required, the data subject will be informed.

In the event that any inaccurate personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

11. ERASURE OF PERSONAL DATA

Individuals have the right to request that Axiom Maths permanently erases any personal data held about them in the following circumstances:

- i. Where the personal data is no longer necessary for the purpose(s) for which it was collected and processed.
- ii. Where consent is withdrawn and there is no other legal basis for the processing.
- iii. Where a data subject objects to the processing of their personal data and there is no overriding legitimate interest to allow the charity to continue doing so.
- iv. Where personal data is being unlawfully processed.
- v. Where there is a legal obligation on Axiom Maths to delete the personal data held.

The Axiom Maths Data Protection Lead will make a decision regarding any application for erasure of personal data and will balance the request against the exemptions provided by law.

All requests for erasure will be complied with and the individual notified within one month unless Axiom Maths has reasonable grounds to refuse the request. This period can be extended by up to two months in the case of complex requests. If additional time is required, the data subject will be informed.

Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

12. RESTRICTION OF PERSONAL DATA PROCESSING

Data Subjects can request Axiom Maths restrict the processing of the personal data it holds about them. If such a request is made, the charity shall reasonably ensure that the personal data is only stored, and no further processing occurs.

If Axiom Maths is required to process the data for statutory purposes or for legal compliance, then the charity shall inform the Data Subject that this processing is expected to take place. This notice will be provided prior to processing.

Where the personal data has been disclosed to third parties, those parties will be informed of the applicable restrictions on processing that shared data (unless it is impossible or would require disproportionate effort to do so).

13. OBJECTIONS TO PERSONAL DATA PROCESSING

An individual has the right to object to the processing of their personal data where such processing is for the purpose of a public interest or for Axiom Maths' legitimate interest.

Where such an objection is made it will be treated as a request for the restriction of processing of personal data. Axiom Maths' Data Protection Lead will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individual, or whether the information is required for the establishment, exercise or defence of legal proceedings.

Where a data subject objects to Axiom Maths processing their personal data for direct marketing purposes, the charity shall cease such processing immediately.

Where a data subject objects to Axiom Maths processing their personal data for scientific and/or historical research and statistical purposes, the data subject may only object to his or her own personal data being processed. Axiom Maths is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

The Axiom Maths Data Protection Lead shall be responsible for notifying the individual of the outcome of their assessment within one calendar month of receipt of the objection. This period can be extended by up to two months in the case of complex requests. If additional time is required, the data subject will be informed.

14. OTHER RIGHTS

Right to Portability

If an individual wants to send their personal data to another organisation, they have a right to request that Axiom Maths provides their information in a structured, commonly used, and machine-readable format, which will be sent to the individual requesting their personal data.

As this right is limited to situations where the charity is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited.

15. PROFILING AND AUTOMATED DECISION MAKING

Data subjects have the right to not be subject to a decision based solely on automated processing, including profiling, of their personal data, which could significantly personally or legally affect them.

Automated processing can only be used if:

1. It is necessary for entering into or for the performance of a contract between the data subject and data controller
2. It is authorised by law
3. It is based on the individual's explicit consent

Where such decisions have a significant or legal effect on data subjects, those data subjects have the right to challenge to such decisions under the UK GDPR.

Currently Axiom Maths does not use profiling or automated decision making as part of its processing of personal data.

16. DATA SECURITY

Axiom Maths will take reasonable steps to ensure that employees will only have access to personal data where it is necessary for them to carry out their duties. Axiom Maths will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

Transferring Personal Data and Communications

Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

Axiom Maths will ensure that where special category personal data or other sensitive information is sent in the post, it shall be able to demonstrate that it was delivered, for example, by using a recorded or tracked delivery service.

Where personal data is to be sent by facsimile the recipient should be informed in advance of the transmission and will be asked to wait by the fax machine as we transfer the data.

Where special category personal data or other sensitive information is to be sent by email, the email will either be sent using a suitable encryption method or the data will be sent in an attached encrypted document and not in the body of the e-mail.

Where personal data is to be transferred in removable storage devices, these devices shall be encrypted. The use of unencrypted removable storage devices is prohibited by Axiom Maths.

The following list includes the most usual reasons that the charity will authorise disclosure of personal data to a third party:

- i. To give a confidential reference relating to a current or former employee, volunteer, or beneficiary
- ii. For the prevention or detection of crime
- iii. For the assessment of any tax or duty
- iv. Where it is necessary to exercise a right or obligation conferred or imposed by law upon the charity (other than an obligation imposed by contract)
- v. For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings)
- vi. For the purpose of obtaining legal advice
- vii. For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress)
- viii. Should concerns be raised by a beneficiary that must be disclosed for safeguarding reasons

Axiom Maths may receive requests from third parties (i.e., those other than the data subject, Axiom Maths, and employees of Axiom Maths) to disclose personal data it holds about beneficiaries, staff, clients, or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or Axiom Maths.

All requests for the disclosure of personal data must be sent to the Axiom Maths' Data Protection Lead, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

Storage

Axiom Maths shall ensure that the following measures are taken with respect to the storage of personal data:

- i. All electronic copies of personal data will be stored securely using passwords, user access rights and where appropriate data encryption:
- ii. All hardcopies of personal data, along with any electronic copies stored on removable storage devices will be stored securely in a locked box, drawer, cabinet, or similar:
- iii. All personal data relating to Axiom Maths' operations, stored electronically, will be backed up on a regular basis.

Where any employee stores personal data on a mobile device (computer, tablet, phone or any other device) that employee must abide by the ICT Acceptable Use policy. The employee shall also ensure that they can provide a secure environment for that device to be used to minimise any risk to the confidentiality, security or integrity of the information.

Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to Axiom Maths' Data Retention Policy.

Use of Personal Data

Axiom Maths shall ensure that the following measures are taken with respect to the use of personal data:

No personal data may be transferred to any employee, partner, contractor, or other party, whether such parties are working on behalf of the charity or not, without the initial authorisation of the Data Protection Lead, in consultation with Axiom Maths' CEO.

Personal data must not be shared informally. If an employee, partner, sub-contractor, or other party working on behalf of the charity requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Protection Lead.

Personal data must always be handled with care and should not be left unattended or available to view by unauthorised employees, partners, sub-contractors, or other parties at any time.

If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

Where the personal data held is used for marketing purposes, it shall be the responsibility of Data Protection Lead to ensure that the appropriate consent is obtained, and that no data subjects have opted out.

IT Security

For further details regarding the security of IT systems, please refer to Axiom Maths' ICT Acceptable Use Agreement. Axiom Maths' Incident Response Strategy outlines how data kept on Axiom Maths' servers / cloud-based storage will be kept secure, and then recovered, in the event of a major incident.

Axiom Maths shall ensure that the following measures are taken with respect to IT and information security:

Axiom Maths requires that any passwords used to access personal data shall have a minimum of 8 characters, composed of a mixture of upper- and lower-case characters, numbers, and symbols. Passwords are not expected to be changed on a regular basis, but users will be expected to change their password if instructed by Axiom Maths.

Under no circumstances should any passwords be written down or shared between any employees, partners, contractors, or other parties working on Axiom Maths' behalf, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

All software (including, but not limited to, applications and operating systems) shall be kept up to date. Axiom Maths' IT provider shall be responsible for installing any and all

security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so.

No software may be installed on any Axiom Maths owned computer or device without the prior approval of Axiom Maths' IT provider.

Where employees or others use online applications that require the use of personal data, the use of that application must be signed off by the Data Protection Lead.

17. ORGANISATIONAL MEASURES

Axiom Maths will ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

All employees, partners, contractors, or other parties working on Axiom Maths' behalf shall be made fully aware of their individual responsibilities and the charity's responsibilities under the UK GDPR and those detailed within this Policy and shall have free access to a copy of this Policy.

Only employees, partners, sub-contractors, or other parties working on Axiom Maths' behalf that need access to, and use of personal data in order to carry out their duties correctly shall have access to personal data held by the charity.

All employees, partners, contractors, or other parties working on Axiom Maths' behalf handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or elsewhere.

Methods of collecting, holding, and processing personal data shall be reviewed regularly (at least annually) and evaluated by Axiom Maths' Data Protection Lead and CEO, to ensure that information is processed appropriately and for the purpose it was collected and not held longer than is necessary.

All personal data held by Axiom Maths shall be reviewed periodically, as set out in Axiom Maths' Data Retention Policy to ensure it has been held in accordance with the retention schedule.

Axiom Maths shall ensure the effective training and understanding of the importance of compliance with Data Protection Laws for all its employees. Axiom Maths shall further ensure refresher training is provided to all employees as necessary and, in any event, no less than once per year. All partners, contractors, or other parties working on behalf of the charity shall ensure that all personnel handling personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and have undergone training in the law of data protection.

The contravention of these rules will be treated as a disciplinary matter.

All employees, partners, contractors, or other parties working on Axiom Maths' behalf who handle personal data will be contractually bound to do so in accordance with the principles of the UK GDPR and this Policy.

All partners, contractors, or other parties working on behalf of the charity handling personal data must ensure that any and all of their employees who are involved in the

processing of personal data are held to the conditions of this Policy and the UK GDPR regulations.

Where any partner, contractor or other party working on behalf of Axiom Maths handles personal data and fails in their obligations under this Policy, that party shall indemnify and will not hold Axiom Maths legally responsible against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

18. TRANSFERRING PERSONAL DATA TO A COUNTRY OUT OF THE EEA/ UK

Axiom Maths may from time-to-time transfer personal data to countries outside of the EEA. The transfer of personal data to a country outside of the EEA shall only take place if one or more of the following applies:

- i. The transfer is to a country, territory, or one or more specific sectors or international organisation, that the European Commission has deemed provides an adequate level of protection for personal data.
- ii. The transfer is to a country or international organisation which provides appropriate safeguards in the form of a legally binding agreement; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the UK GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.
- iii. The transfer is made with the informed and explicit consent of the relevant data subject(s)
- iv. The transfer is necessary for the performance of a contract between the data subject and Axiom Maths (or for pre-contractual steps taken at the request of the data subject).
- v. The transfer is necessary for important public interest reasons.
- vi. The transfer is necessary for the conduct of legal claims.
- vii. The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent.

19. DATA BREACH NOTIFICATION

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Lead must ensure that the Information Commissioner's Office is informed without delay, and in any event, within 72 hours after having become aware of the breach.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Lead must ensure that all affected data subjects are informed of the breach directly and without delay.

Data breach notifications shall include, at minimum, the following information:

- i. The categories and approximate number of data subjects affected
- ii. The categories and approximate number of personal data records affected
- iii. The name and contact details of Axiom Maths' Data Protection Lead
- iv. The likely consequences of the breach
- v. Details of the measures taken, or proposed to be taken, by Axiom Maths to address the breach including, where appropriate, measures to mitigate the possible effects to those data subjects.

20. IMPLEMENTATION OF POLICY

This Policy shall be effective from 1 September 2023. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

21. COMPLAINTS

Axiom Maths aims to comply fully with its obligations under the UK GDPR. If you have any questions or concerns regarding Axiom Maths' management of personal data including your subject rights, please contact the Data Protection Lead (info@axiommaths.com) who is responsible for ensuring Axiom Maths is compliant with the UK GDPR.

If you have any questions or concerns regarding Axiom Maths' management and use of personal data including your subject rights, please contact the Data Protection Lead who is responsible for ensuring Axiom Maths is compliant with the UK GDPR.

If you feel that your questions/concerns have not been dealt with adequately on any data protection matter, please get in touch directly with Axiom Maths' CEO (david.thomas@axiommaths.com). If you are still not satisfied, or your concern is regarding the CEO, then please get in touch with Axiom Maths' Board of Trustees (dan.abramson@axiommaths.com)

If you are not satisfied with the assistance that you get or if you feel your complaint has not been resolved and you feel that a formal complaint needs to be made, then you can contact the ICO. Please visit their website (www.ico.org.uk) for more information. Alternatively, contact can be made directly, addressed to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5A (telephone: 0303 123 1113).

22. CONTACT – DPO INFORMATION

Axiom Maths is a registered Data Controller with registration number ZB345801.

The Axiom Maths Board of Trustees is ultimately accountable for ensuring that Axiom Maths complies with all relevant legislation including data protection. Data protection sits under the remit of the Axiom Maths Chief Executive Officer.

The Axiom Maths Data Protection Lead is responsible for the overall coordination of data protection including overseeing responses to Subject Access Requests, data breaches and Data Protection Impact Assessments.



All staff are made aware of this policy and their duties under GDPR as part of their induction to Axiom Maths. In addition, regular training is provided to staff, in particular those for whom data protection is of particular relevance to their role.

If anyone has any concerns or questions in relation to this policy, they should contact the Axiom Maths Data Protection Lead via info@axiommaths.com.