SIR ROBERT PATTINSON ACADEMY

DATA PROTECTION POLICY

Date Reviewed in School: June 2026

Date Approved by Trustees: 20 July 2026

Review Date: June 2029

DATA PROTECTION POLICY

SECTION 1: PRELIMINARY POINTS

PURPOSE OF THIS POLICY

This procedure supports our information governance framework and defines data protection from the Academy's perspective. It includes what the law requires in this respect, principally under the Data Protection Act 2018,the UK General Data Protection Regulation (**UK GDPR**), and the Data (Use and Access) Act 2025 (**DUAA**).

You must read this policy because it gives important information about:

- the data protection principles with which the Academy must comply;
- what is meant by personal information (or data) and special categories of data (previously known as sensitive data);
- how we gather, use and (ultimately) delete personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information we gather and use about individuals, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- individuals' rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

INTRODUCTION

The Academy processes personal information relating to students, parents and carers, staff, Trustees, volunteers, visitors, contractors, job applicants, and other stakeholders for a number specific lawful purposes. This is set out in the Academy's Privacy Statement, which all employees should be familiar with. In carrying out these activities, the Academy will usually act as a data controller. In some limited circumstances, the Academy may also process information on behalf of another controller, in which case it will comply with the applicable processor obligations.

This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our students and workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information, and how (and when) we delete that information once it is no longer required.

The Academy is an organisation that processes personal information.

Therefore, we are registered with the Information Commissioner on the Data Protection Public Register. This means we have told the Information Commission that we process personal information and how we do this, and they have issued us with registration numbers so they can identify us, as follows:

	Registration Number	Registered
Sir Robert Patterson Academy	Z2923046	14.11.2011

DATA PROTECTION OFFICER

The implementation of this Policy is overseen by the Academy's Data Protection Officer (**DPO**). The DPO is responsible for informing and advising the Academy and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Academy's policies.

If you have any questions, concerns, or requests in relation to this policy, you should contact the DPO.

SCOPE

The DPO is contactable via ltimbrell@srpa.co.uk or enquiries@srpa.co.uk.

This policy applies to all personal information processed by the Academy in whatever capacity and in whatever media.

Staff should refer to the Academy's Privacy Statement and, where appropriate, to its other relevant policies including in relation to Internet, Email and Communications, Social Media, Records Retention and Information Security.

We will review and update this policy regularly in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

The legal definition of 'data' under the UK GDPR is complicated. However, for the purposes of this Policy, you should assume that all information concerning an identifiable individual is data.

SECTION 2: THE LEGAL FRAMEWORK

WHAT IS THE UK GDPR?

The UK GDPR establishes a framework of rights and duties which are designed to safeguard personal and special categories of data (what used to be called 'sensitive data'). It came into force on the 25th May 2018 and replaced, among other

things, the Data Protection Act 1998.

The UK GDPR seeks to balance the legitimate needs for organisations like ours to collect and use personal data for business and other purposes against the rights of individuals to respect for the privacy of their personal information.

DEFINITIONS

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
Special categories information	(previously known as 'sensitive personal data' under the previous legislation) means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

THE PRINCIPLES OF THE UK GDPR

The Academy will comply with the principles relating to processing of personal data set out in the UK GDPR, which requires personal data to be:

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);
- Collected for specified, explicit and legitimate purposes (purpose limitation);
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed (data minimisation);
- Accurate and, where necessary, kept up to date (accuracy);
- Kept for no longer than is necessary for the purposes for which it is processed (storage limitation);
- Processed in a way that ensures it is appropriately secure (security, integrity and confidentiality);
- Not transferred to another country without appropriate safeguards in place (transfer limitation); and
- Handled in a way that respects the rights of data subjects and allows them to exercise those rights (data subject rights and requests).
-

SECTION 3: THE INFORMATION COMMISSIONER'S OFFICE (ICO)

WHO ARE THE ICO?

The ICO is the UK's independent authority who upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Information Commissioner has responsibilities around the Freedom of Information Act as well as data protection.

WHAT ARE THE ICO RESPONSIBLE FOR?

The UK GDPR makes the ICO responsible for:

- Promoting good practice in handling personal data and giving advice and guidance on data protection;
- Keeping a register of organisations who process information and data;
- Helping to resolve disputes to determine if organisations have complied with the UK GDPR
- Taking action to enforce compliance where necessary;
- Bringing prosecutions for offences committed under the UK GDPR.

Importantly, our staff have personal liability in certain circumstances under the UK GDPR. It is therefore critical that the highest standards of data protection are applied

throughout the Academy.

SECTION 4: THE RIGHTS OF INDIVIDUALS

WHAT ARE THE RIGHTS OF INDIVIDUALS FOR WHOM WE HOLD INFORMATION?

You (in common with other data subjects) have the following rights in relation to your personal information:

- to be informed about how, why and on what basis that information is processed—see the Academy's Privacy Statement;
- to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request;
- to have data corrected if it is inaccurate or incomplete;
- to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as '*the right to be forgotten'*);
- to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and
- to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).
- to complain if you are unhappy with how we have processed your personal data (see Section 9 below).

If you wish to exercise any of your rights, please contact the DPO. If another individual, such as one of our clients, expresses an interest in exercising their rights, please refer them to the DPO.

REQUESTS FROM STUDENTS

Children have the same rights as adults over their personal data which they can exercise as long as they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility may usually exercise the child's data protection rights on their behalf.

If a member of staff considers that there may be an issue with a student's competency, they should discuss this with the DPO.

The ability of young people to understand and exercise their rights is likely to develop or become more sophisticated as they get older. As a general guide, a child of 12 or older is expected to be mature enough to understand the request they are making. A child may, of course, be mature enough at an earlier age or may lack sufficient maturity until a later age, and so requests should be considered on a case by case basis.

Accordingly, if a student exercises a right under the UK GDPR and they have competency, we must both support the student in doing so and comply with any request they make, unless there is a legal reason why we cannot do so.

REQUESTS FROM PARENTS

Parents do not have an automatic right to access to their child's personal information. We can only share information with parents where we are legally obliged to do so, or where we have the student's consent, or there is some other legal justification (such as the student is not competent to give consent).

Because we are an Academy, parents do not have a legal right to access their child's education record, unless their child has given consent.

SUBJECT ACCESS REQUESTS

By law, individuals have a right to make a subject access request (SAR) to gain access to personal information that the Academy holds about them. A SAR may be made verbally or in writing, but we may be able to respond to requests more quickly if they are made in writing.

A SAR may include a request for:

- confirmation that their personal information is being processed;
- access to a copy of the personal information;
- the purposes of the processing;
- the categories of personal information concerned;
- the recipients or categories of recipients to whom the information has been or will be disclosed;
- the period for which the information will be stored, or the criteria used to determine that period;
- the source of the information, if not obtained from the individual;
- information about relevant rights, including rectification, erasure, restriction, objection and complaint rights;
- details of safeguards where personal information is transferred outside the UK; and
- information about automated decision-making or profiling, if applicable.

If staff receive a SAR in any form, they must immediately forward it to the DPO. Staff should not delay because time limits apply even where a request is made during school holidays or to a member of staff who is not the DPO.

The Academy may ask for information reasonably required to confirm the requester's identity or to clarify the request. It may be able to respond more quickly if the request is made in writing and includes the requester's name, correspondence address, contact number, email address and details of the information requested.

The Academy will respond without undue delay and within the statutory time limit, usually one month from receipt of the request or, where required, receipt of information needed to confirm identity. Where a request is complex or numerous, the Academy may extend the response period by a further two months. If an extension is needed, the Academy will inform the individual within one month and explain why the extension is necessary.

The Academy will usually provide the information free of charge. If a request is manifestly unfounded or excessive, the Academy may refuse to act on it or charge a reasonable fee, where permitted by law. If the Academy refuses a request, it will explain why and inform the individual of their right to complain to the ICO and to seek to enforce their rights through the courts.

The Academy may withhold or redact information where an exemption applies. This may include, for example, information which would reveal another person's personal information, or information subject to confidentiality.

SECTION 5: INFORMATION SECURITY

IN GENERAL

All staff must familiarise themselves with and adhere to the guidance set out in **Appendix 1** of this Policy.

DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

Where processing is likely to result in a high risk to an individual's data protection rights (eg where the Academy is planning to use a new form of technology or marketing strategy), we will, before commencing the processing, carry out a DPIA to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal information.

Any DPIA should be overseen by the DPO.

SHARING PERSONAL INFORMATION

The Academy will not share personal information with third parties unless there is a lawful basis for doing so and appropriate safeguards are in place. Staff must only share the minimum personal information necessary for the relevant purpose.

There will be circumstances where the Academy may be required or permitted to share personal information. These include, but are not limited to, situations where:

- there is an issue involving a student, parent or carer which puts the safety of students, staff or others at risk;
- the Academy needs to liaise with safeguarding partners, local authorities, health bodies, other schools, regulators, law enforcement agencies or emergency services;
- suppliers or contractors need information to provide services to the Academy, staff or students;
- the Academy is required by law, court order or regulatory requirement to share information; or
- sharing is necessary to protect someone's vital interests or respond to an emergency.

Where staff are unsure whether information may be shared, they must seek advice from the DPO before sharing it unless there is an immediate safeguarding or emergency reason requiring urgent action.

WHAT IF A THIRD PARTY ASKS YOU TO SHARE INFORMATION?

Sometimes we may be asked by a third party to share information about an individual or group of individuals e.g. the police, local authority or another school. Sometimes this is fine and sometimes it is not.

Staff should not be expected to make difficult data sharing decisions without support. If the Academy's Privacy Statement or procedures do not clearly permit the sharing, staff must seek approval from the DPO before sharing the information. Staff should record what information was shared, with whom, when, why and the lawful basis relied on, where required by the Academy's procedures.

DISCLOSURES TO THE POLICE

Disclosures to the Police are not compulsory except in cases where served with a Court Order requiring information. Requests from the Police for access to information must be made in writing as specified under the DPA. The Police must complete a form, which should then be approved by the Head Teacher.

Employees must not release information to the Police over the telephone.

In cases where a request from the Police has been made but a Court Order is not served, consideration must be given to the implications of disclosure before any action is taken.

The Academy may be required to provide an explanation for any disclosure of the data subject's personal information at a later date and must be able to provide justifiable reasons for doing so e.g. where the Academy believes that failure to release the information would prejudice an investigation.

SUPPLIERS, CONTRACTORS AND PROCESSORS

Where the Academy uses external organisations to process personal information on its behalf, appropriate due diligence and contractual arrangements must be in place before processing starts. The Academy will only appoint suppliers or contractors that can provide sufficient guarantees that they will comply with UK data protection law and keep personal information secure.

In particular, contracts with external organisations must provide that:

- the organisation may act only on the written instructions of the Academy;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of the Academy and under a written contract;
- the organisation will assist the Academy in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will assist the Academy in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to the Academy as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide the Academy with whatever information it needs to ensure that both parties are meeting their data protection obligations, and tell the Academy immediately if it is asked to do something that infringes data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is amended, the relevant staff must seek approval of its terms by the DPO.

INTERNATIONAL TRANSFERS

Staff must not transfer personal information to, or make personal information accessible to, a separate organisation located outside the UK without first consulting the DPO. The

DPO will consider whether the transfer is restricted under the UK GDPR or other applicable data protection legislation, and will identify whether there is a lawful basis for the transfer, such as an adequacy decision, appropriate safeguards, an exception, or another lawful transfer mechanism.

This includes the use of cloud services, overseas suppliers, remote access arrangements, overseas trips and any other situation where personal information may be accessed from outside the UK.

INFORMATION SECURITY MEASURES

The Academy will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These include:

- making sure that, where possible, personal information is pseudonymised or encrypted;
- prohibiting all users from using USB and other external storage devices for transferring or storing student data;
- the use of external storage devices may be permitted on the IT system under strict conditions; Data is encrypted, approved and checked by the IT staff, and used for subjects such as photography and exams.
- permitting staff remote access to school systems in a safe and secure way and ensuring that personal data is not transferred to or processed via personal devices;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
- regularly training staff on data protection awareness and our policies;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Where the Academy uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- the organisation may act only on the written instructions of the Academy;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;

- sub-contractors are only engaged with the prior consent of the Academy and under a written contract;
- the organisation will assist the Academy in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will assist the Academy in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to the Academy as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide the Academy with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Academy immediately if it is asked to do something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the DPO.

STORAGE AND RETENTION

Personal information (and sensitive personal information) will be kept securely in accordance with the Academy's Information Security Policy, set out in **Appendix 3.**

Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow the Academy's Records Retention Policy which sets out the relevant retention period, or the criteria that should be used to determine the retention period.

Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

DATA BREACHES

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;

- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

In the event of a data breach, the Academy will:

- make the required report of the data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals;
- notify the affected individuals if the data breach is likely to result in a high risk to their rights and freedoms and notification is required by law; and
- will follow the personal data breach procedure set out in **Appendix 2**.

You must notify the DPO immediately if you become aware of a data breach, or potential data breach, even if there are no apparent consequences. This means notification to the DPO must be made straight away, and in any event within one working hour of discovering the breach. Notification must be made personally – i.e. you must find the DPO, or deputy, and tell them. Sending an email is not sufficient. If the DPO is not available, you must report directly to the Head Teacher.

SECTION 6: TYPES OF PROCESSING

BIOMETRIC DATA

We employ the use of biometric identification technology. Accordingly, we are required to process and retain any information gathered by such means in line with the terms of the Data Protection Act 2018, the Protection of Freedoms Act 2012, the UK GDPR, and applicable DfE guidance.

Where we process biometric data, we will;

1. Maintain a record of the technology/system used to gather and store the data.
2. Ensure that consent is sought from at least one parent for each student whose biometric information will be collected.
3. Ensure that biometric information is retained in line with our retention schedule.

Should a student or parent wish to withdraw or withhold their consent to the processing of their biometric data, the academy should provide a suitable alternative means of identification which does not penalise either the student or their parent(s).

Further information on academies obligations in relation to the processing of biometric

information can be found in the DfE's guidance document.

CCTV

Where the Academy uses CCTV, it will use CCTV in accordance with data protection law and applicable ICO guidance. CCTV may be used in various locations around the Academy site for purposes including site security, safeguarding, the prevention and detection of crime, and the safety of students, staff, visitors and the wider Academy community.

The Academy does not usually need to ask individuals' permission to use CCTV, but it will make clear where individuals are being recorded. Cameras will be clearly visible where appropriate and accompanied by prominent signs explaining that CCTV is in use. Cameras will be positioned appropriately and will not be used in areas where individuals would reasonably expect privacy, unless exceptional circumstances justify this and appropriate safeguards are in place.

Access to CCTV footage will be restricted to authorised individuals. Footage will only be disclosed where there is a lawful basis to do so, for example to law enforcement agencies, safeguarding agencies, insurers, legal advisers or regulators where appropriate. CCTV footage will be retained in accordance with the Academy's retention schedule, unless it is required for an investigation or another lawful purpose.

PHOTOGRAPHS AND VIDEOS

Any enquiries about the CCTV system should be directed to the DPO As part of Academy activities, the Academy may take photographs and videos of students, staff, visitors and other individuals.

The Academy may use photographs and videos for purposes including educational activities, displays, record-keeping, newsletters, the Academy website, social media, prospectuses, marketing materials, school trips, performances, sports events, identity systems and other Academy communications.

Where consent is relied upon, the Academy will clearly explain the proposed use of the photograph or video and obtain appropriate consent from the parent or carer, student or member of staff, as applicable. Consent can be refused or withdrawn at any time. Where consent is withdrawn, the Academy will stop further use of the relevant image and will take reasonable steps to remove it from future publications, although it may not always be possible to recall material already published.

The Academy will avoid publishing unnecessary identifying information alongside images, particularly images of students. Where safeguarding concerns apply, staff must seek advice from the Designated Safeguarding Lead and the DPO before any image is used or disclosed.

Photographs and videos taken by parents and carers at Academy events for their own personal use are not generally covered by data protection law.

However, for safeguarding reasons, the Academy may ask parents and carers not to share images or videos publicly, including on social media, where those images or videos include other students, unless the relevant individuals or parents/carers have agreed.

ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence tools, including generative AI tools and chatbots, are now widespread and easy to access. The Academy recognises that AI may have uses in education and administration, but also poses risks to personal information, confidential information, safeguarding and intellectual property.

Staff, Trustees, volunteers, contractors and students must not enter personal information, special category information, safeguarding information or any other confidential Academy information into any unauthorised AI tools or chatbots. AI tools may only be used where authorised by the Academy and in accordance with any applicable Academy guidance, privacy notice, DPIA, safeguarding requirements, procurement process and supplier approval process.

If personal, sensitive, safeguarding or confidential information is entered into an unauthorised AI tool, the Academy will treat this as a potential data breach and will follow the data breach procedure in this policy.

SECTION 7: COMPLAINTS

The Academy takes any complaint about how it collects, uses, stores, shares or otherwise processes personal information seriously.

If an individual believes that the Academy's processing of their personal information is unfair, misleading, inappropriate or otherwise in breach of data protection law, they should raise this with the Academy in the first instance by contacting the DPO.

Upon receiving a data protection complaint, and in accordance with DUAA, the Academy will:

- acknowledge receipt of the complaint within 30 days of receiving it;
- take appropriate steps to respond to the complaint without undue delay;
- make appropriate enquiries based on the circumstances of the complaint;
- keep the complainant informed on the progress of the investigation where appropriate; and
- inform the complainant of the outcome without undue delay.

If you remain dissatisfied after receiving our response, you have the right to complain to the ICO.

SECTION 8: TRAINING & MONITORING

TRAINING

All staff and Trustees will receive data protection training as part of the induction process. Data protection will also form part of continuing professional development where changes to legislation, guidance, Academy systems or Academy processes make it necessary.

Additional training may be required for staff who regularly handle sensitive personal information, safeguarding information, SARs, CCTV footage, biometric information, AI tools, records retention or high-risk processing activities.

MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy and recommending updates where required. This policy will be reviewed at least annually and approved by the Board of Trustees, or sooner where required by changes in law, guidance, ICO expectations, DfE guidance, Academy practice, systems or risk profile.

Where this policy does not cover biometric data, approval may be delegated where permitted by the Academy's governance arrangements. Where biometric data is covered, the Academy should ensure the appropriate approval route is followed.

OTHER POLICIES

This policy should be read in conjunction with the Academy's other policies and notices relating to data protection, including but not limited to:

- Privacy Statement and privacy notices;
- Internet, Email and Communications Policy;
- Social Media and Acceptable Use Policies; and
- Safeguarding and Child Protection Policy;

SECTION 9: YOUR OBLIGATIONS

THIS IS PARTICULARLY IMPORTANT

You will have access to the personal information of other members of staff and students in the course of your employment or engagement. The Academy expects you to help meet its data protection obligations to those individuals at all times.

For example, you should be aware that all data subjects enjoy the rights listed above.

In respect of personal information to which you have access, you must:

- only access the personal information that you have authority to access, and only for authorised purposes;
- only allow other Academy staff to access personal information if they have appropriate authorisation;
- do not write down (in electronic or hard copy form) opinions or facts concerning individuals which it would be inappropriate to share with that data subject;
- only allow individuals who are not Academy staff to access personal information if you have specific authority to do so from the DPO;
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Academy's Information Security Policy);
- not enter personal information into unauthorised AI tools or chatbots;
- not remove personal information, or devices containing personal information (or which can be used to access it), from the Academy's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
- not store personal information on local drives or on personal devices that are used for work purposes.

You should contact the DPO if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the special conditions being met;
- any data breach (defined below);
- access to personal information without the proper authorisation;
- personal information not kept or deleted securely;
- removal of personal information, or devices containing personal information (or which can be used to access it), from the Academy's premises without appropriate security measures being in place;
- use of personal information in an unauthorised AI tool; or
- any other breach of this policy or of any of the data protection principles (set out above).

SECTION 10: CONSEQUENCES OF FAILURE TO COMPLY

The Academy takes compliance with this policy very seriously. Failure to comply with the policy:

- puts at risk the individuals whose personal information is being processed; and
- carries the risk of significant civil and criminal sanctions for the individual and the Academy; and
- may, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

APPENDIX 1

Information Security Principles

GENERAL PRINCIPLES

All Academy information, especially that relating to our students and staff, must be treated as confidential and be protected from loss, theft, misuse or inappropriate access or disclosure.

Staff should discuss with line managers the security arrangements which are appropriate and in place for the type of information they access in the course of their work.

Staff should ensure they attend any information security training they are invited to unless otherwise agreed by line managers.

Academy information must only be used in connection with work being carried out for the Academy and not for other commercial or personal purposes.

INFORMATION MANAGEMENT

Information gathered should not be excessive and should be adequate, relevant, accurate and up to date for the purposes for which it is to be used by the Academy.

Information will be kept for no longer than is necessary in accordance with the Academy's Retention Policy. All confidential material that requires disposal must be shredded or, in the case of electronic material, securely destroyed, as soon as the need for its retention has passed.

HUMAN RESOURCES INFORMATION

Given the internal confidentiality of personnel files, access to such information is limited to members of the SLT, or others as determined by the head teacher. Except as provided in individual roles, other staff are not authorised to access that information.

Staff may ask to see their personnel files in accordance with the relevant provisions of the UK GDPR and are referred to the Academy's Privacy Statement for more information on their rights.

ACCESS TO OFFICES AND INFORMATION

Office doors must be kept secure at all times and visitors must not be given keys or access codes. Students must not be left in offices unattended.

Documents containing confidential information and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by, eg through office windows.

Visitors should be required to sign in at reception, accompanied at all times and never be left alone in areas where they could have access to confidential information.

Wherever possible, visitors should be seen in meeting rooms. If it is necessary for a member of staff to meet with visitors in an office or other room which contains Academy information, then steps should be taken to ensure that no confidential information is visible.

At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing confidential information must be securely locked away.

COMPUTERS AND IT

- Use password protection and encryption where available on Academy systems to maintain confidentiality. Students should not be left alone in rooms where there are unlocked computers.
- Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis. Passwords should not be written down or given to others.
- Computers and other electronic devices should be locked when not in use to minimise the risk of accidental loss or disclosure.
- Confidential information must not be copied onto removeable storage devices unless preapproved by the IT staff and under specific conditions. Data copied onto any of these devices must be encrypted and should be deleted as soon as possible and stored on the Academy's computer network in order for it to be backed up.

- Personal data relating to staff or students should ONLY be processed via the Academy's computer network.
- All school resources including classroom resources should be stored on the IT system to encourage good practice and prevent data loss.
- Any resources stored on personal devices through use of Frog should be deleted once transferred to the Academy network.
- All electronic data must be securely backed up at the end of each working day via the Academies backup policy.
- Staff should ensure they do not introduce viruses or malicious code on to Academy systems. Software should never be installed or downloaded from the internet.. Staff should contact the IT department for review of this software and if approved only IT staff should download and install software to ensure compliance and in keeping with the Academy's IT Acceptable use and Email Policy.

COMMUNICATIONS AND TRANSFER

Staff should be careful about maintaining confidentiality when speaking in public areas.

Confidential information should be marked 'confidential' and circulated only to those who need to know the information in the course of their work for the Academy.

Confidential information must not be removed from the Academy's offices without permission from a member of SLT except where that removal is temporary and necessary.

In the limited circumstances when confidential information is permitted to be removed from the Academy's offices, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained. Staff must ensure that confidential information is:

- not transported in see-through or other un-secured bags or cases;
- not read in public places (e.g. waiting rooms, cafes, trains); and
- not left unattended or in any place where it is at risk (e.g. in conference rooms, car boots, cafes).

Postal, document exchange (DX), fax and email addresses and numbers should be checked and verified before information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

All sensitive or particularly confidential information should be encrypted before being sent by email, or be sent by tracked DX or recorded delivery.

Sensitive or particularly confidential information should not be sent by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

HOME WORKING

Staff should not take confidential or other information home without the permission of a member of SLT and only do so where satisfied appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information.

In the limited circumstances in which staff are permitted to take Academy information home, staff must ensure that:

- confidential information must be kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- all confidential material that requires disposal must be shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed.

Staff should not store confidential information on personal devices (PCs, laptops or tablets).

TRANSFER TO THIRD PARTIES

Third parties should only be used to process Academy information in circumstances where written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings.

Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the DPO for more information.

REPORTING BREACHES

All staff have an obligation to report actual or potential data protection compliance failures to the DPO. This allows the Academy to:

- investigate the failure and take remedial steps if necessary; and
- make any applicable notifications.

For more information, see the Academy's Data Protection Policy.

CONFIDENTIALITY

The Academy is a controller and processor for the purposes of the UK GDPR and is obliged to keep personal data secure and process it fairly and lawfully.

The individuals for whom the Academy collects and processes personal information have a right to believe and expect that the information they provide will be used for the purposes for which it was originally given, and not released to others without their consent. Everyone who is employed by or who volunteers for the Academy must safeguard the integrity and confidentiality of, and access to personal or sensitive information.

APPENDIX 2

Data Breach Response Principles

PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO and should be read alongside Section 5 of this policy.

On finding or causing a breach or potential breach, the staff member, Trustee, volunteer, contractor or data processor must immediately notify the DPO in accordance with the internal reporting requirement in this policy, and in any event within one working hour of becoming aware of the breach or potential breach.

The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal information has been accidentally or unlawfully:

- lost;
- stolen;
- destroyed;
- altered;
- disclosed or made available where it should not have been; or
- made available to unauthorised people.

Staff and Trustees will co-operate with the investigation, including allowing access to information and responding to questions. The investigation will not be treated as a disciplinary investigation unless and until the Academy decides that disciplinary issues need to be considered separately.

If a breach has occurred or is likely to have occurred, the DPO will alert the Head Teacher and the Chair of Trustees, unless it is inappropriate to do so in the circumstances.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members, IT support providers or data processors should assist the DPO where necessary, and the DPO should take external advice when required.

The DPO will assess the potential consequences, based on seriousness and likelihood, before and after any mitigation steps have been implemented.

The DPO will decide whether the breach must be reported to the ICO and whether affected individuals must be notified. The DPO may use ICO guidance, risk assessment tools or external advice when making this decision.

The DPO will document the decision, whether or not the breach is reported to the ICO or individuals, in case the decision is later challenged by the ICO or an affected individual. Documented decisions will be stored [insert location of breach records].

Where the ICO must be notified, the DPO will do so via the ICO's reporting process within 72 hours of the Academy becoming aware of the breach, where possible. The report will include, where available:

- a description of the nature of the personal data breach, including the categories and approximate number of individuals concerned and personal data records concerned;
- the name and contact details of the DPO;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to deal with the breach and mitigate possible adverse effects.

If all details are not yet known, the DPO will report as much information as possible within 72 hours and provide further information as soon as possible thereafter.

Where the Academy is required to communicate with individuals whose personal information has been breached, the DPO will tell them in clear and plain language. The notification will set out the nature of the breach, the name and contact details of the DPO, the likely consequences, and the measures taken or proposed to deal with the breach and mitigate adverse effects.

The DPO will consider whether to notify any relevant third parties who can help mitigate loss or risk to individuals, for example the police, insurers, banks, credit card companies, safeguarding partners or IT providers.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the facts and cause, effects, action taken to contain it and action taken to reduce the risk of recurrence, such as process changes or further training.

The DPO and Head Teacher will meet as soon as reasonably possible to review what happened and how it can be stopped from happening again. The DPO and Head Teacher will also periodically assess recorded data breaches to identify any trends or patterns requiring action by the Academy.

ACTIONS TO MINIMISE THE IMPACT OF DATA BREACHES

The precise response will depend on the circumstances. Possible actions may include:

- recalling an email sent in error;
- asking unintended recipients to delete information and confirm deletion in writing;

- asking IT support to remove information from systems or prevent further access;
- carrying out internet searches or checks to see whether information has been made public;
- contacting website owners, administrators or platforms to request removal of information;
- informing the Designated Safeguarding Lead where safeguarding information is compromised;
- reviewing whether safeguarding partners, police or other agencies should be informed;
- resetting passwords or access permissions;
- disabling compromised accounts or devices;
- providing further staff training; and
- updating policies, procedures, systems or controls.

Examples of breaches which may require specific consideration include sensitive information being disclosed via email, safeguarding records being sent to the wrong person, details of pupil premium interventions being published, non-anonymised pupil exam results or staff pay information being shared inappropriately, an unencrypted laptop being stolen or hacked, a cashless payment provider being hacked, hardcopy reports being sent to the wrong families, CCTV footage being disclosed without authorisation, or personal information being entered into an unauthorised AI tool.

APPENDIX 3

Records Retention Principles

The UK GDPR states that data should not be kept for longer than necessary for the purpose for which it is held. Therefore, there are no definitive rules for how long data should be held. Each situation should be dealt with on its own merit, but retention records should be justified.

As a general rule, however, the Academy will hold data, including personal and special categories of data (formally, 'sensitive data'), for the following minimum periods, which may be extended where circumstances means it is fair and lawful to do so:

Data Type	Indicative retention period	Start time
Personnel Records		
Application forms and interview notes for unsuccessful candidates	6 months	Date decision communicated
Personnel files and training records (including disciplinary records and working time records)	3 years	Effective date of termination
Records of unfounded allegations of a child protection nature	10 years (unless malicious)	Date notice of allegation received
Original DBS disclosure	6 months	Date of disclosure
Evidence of DBS disclosure	Keep for entirety of employment and for 6 years thereafter	
Wage/salary records (including overtime, bonuses and expenses)	6 years	
Statutory Maternity Pay (SMP) records	3 years	End of tax year to which record relates
Parental leave records	3 years	Date of birth of child
Statutory Sick Pay (SSP) records	3 years	Effective date of termination
Income tax and National Insurance returns/records	7 years	End of tax year to which record relates

National Minimum Wage Records	3 years	end of the pay reference period following the one that the records cover
Pensions scheme and member records	6 years	Effective date of termination
Student information		
Enrolment forms, transfer forms, reports, exam results, correspondence and other notes on file	7 years	Date student attains age of 18
Health and Safety		
Staff accident records	4 years	Date of last entry
Records of any reportable death, injury, disease or dangerous occurrence	3 years	After date of report made
Accident/medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years	Date of last entry
Miscellaneous		
Accounting records (cash books, invoice receipts etc)	6 years	From end of financial year to which record relates