SIR ROBERT PATTINSON ACADEMY

DATA PROTECTION and GDPR POLICY

Date Reviewed in School: October 2021

Date Approved by Governors: 8 November 2021

Review date: September 2024

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 and the General Data Protection Regulation (**GDPR**), the EU law which replaced the Data Protection Act 1998 as from the 25th May 2018.

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, eg 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.

The implementation of this Policy is overseen by the Data Protection Officer, to whom you should address all queries or concerns.

INTRODUCTION

The Academy obtains, keeps and uses personal information (also referred to as data) about our students, job applicants and about current and former employees, governors 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.

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	Expiry Date
Sir Robert Pattinson Academy	Z2923046	14.11.2011	13.11.2020

OVERSEEING OFFICER

The Academy's Data Protection Officer (**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 or comments about the content of this policy or if you need further information, you should contact the DPO.

SCOPE

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 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 GDPR?

The 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 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 the 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;
sensitive personal information	(known as 'special categories of personal data' under the GDPR) 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 GDPR

The Academy will comply with the following data protection principles when processing personal information:

- we will process personal information lawfully, fairly and in a transparent manner;
- we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
- we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
- we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
- we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
- we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

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 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 completed with the GDPR
- Taking action to enforce compliance where necessary;
- Bringing prosecutions for offences committed under the GDPR.

Importantly, our staff have personal liability in certain circumstances under the 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).

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 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.

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.

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 worry about making these decisions. If everyone follows the procedures in place it will be clear when this is acceptable and when it is not. Our Privacy Statement details any information we may already know we intend to share and who with, so it may be clear from checking this if you should share the data being requested. However, if this is not clear and you are not sure then you must seek approval before sharing the information being requested. Send requests to the DPO.

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 staff form using USB and other external storage devices for transferring or storing student data;
- 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 2.**

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.

The Academy will:

- make the required report of a 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; and
- notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

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: 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 (eg 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 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;
- any other breach of this policy or of any of the data protection principles (set out above).

SECTION 7: 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 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 floppy disk, removable hard drive, CD or DVD or memory stick / flash-drive without the express permission of the head teacher. Data copied onto any of these devices 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 ICT 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.
- Staff should ensure they do not introduce viruses or malicious code on to Academy systems. Software should not be installed or downloaded from the internet without it first being virus checked. Staff should contact the IT department for guidance on appropriate steps to be taken to ensure compliance and refer to the Academy's IT 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 (eg waiting rooms, cafes, trains); and
- not left unattended or in any place where it is at risk (eg 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 home computers (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.

OVERSEAS TRANSFER

There are restrictions on international transfers of personal data. Staff must not transfer personal data outside the EEA (which includes the EU, Iceland, Liechtenstein and Norway), such as on school trips, without first consulting the DPO.

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 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. You can share confidential information without consent if it is required by law, or directed by a court, or if the benefits to a child or young person that will arise from sharing the information outweigh both the public and the individual's interest in keeping the information confidential.

APPENDIX 2

Records Retention Principles

The 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
Safeguarding files	10 years	Date student attains age of 26
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