General Data Protection Regulations (GDPR) Policy

The Rushmere Academy

September 2025

PERSON RESPONSIBLE FOR POLICY:	***MICHELLE HARVEY***
APPROVED:	***GABRIELLE BARTON***
SIGNED:	***MICHELLE HARVEY*** ***GABRIELLE BARTON***
TO BE REVIEWED:	***SEPTEMBER 2026***

UKPRN: 10044130 | Legal Address: 20 Francis Street, Northampton, NN1 2NZ

Tel: 01604 635586 / 07729090459

The Rushmere Academy will comply with all statutory requirements under the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) by registering all personal data and by taking all reasonable steps to ensure the accuracy and confidentiality of such information.

The Rushmere Academy will appoint a Director/Officer with overall responsibility for Data Protection (DPO) and register with the Information Commissioners Office.

The Rushmere Academy will assess, and document, the status of each organisation with whom they work in respect of all the personal data and processing activities you carry out.

The Rushmere Academy will seek the permission of individuals to collect, control and process personal data and explain to them how this data will be used**.**

The Data Protection Act protects individual's rights concerning information about them. Anyone processing personal data must comply with the eight principles of good practice.

Data must :-

- Be processed fairly and lawfully.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner compatible with the purpose.
- Be adequate, relevant and not excessive for the purpose.
- Be accurate and up-to-date.
- Not be kept for longer than necessary for the purpose and observe the rights of individuals to have data erased.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised processing, and accidental loss, damage or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data, except in specified circumstances.

Staff Responsibilities

All staff shall:

- Ensure that all personal information which they provide to The Rushmere Academy in connection with their employment is accurate and up-to-date.
- Inform The Rushmere Academy of any changes to information, for example, changes of address.
- Check the information which The Rushmere Academy shall make available from time to time, in written or automated form, and inform Rushmere of any errors or, where appropriate, follow procedures for updating entries on computer forms.
- When staff hold or process information about students, colleagues or other data subjects (for example students' course work, pastoral files, references to other academic institutions, or details of personal circumstances), they should comply with the Data Protection Guidelines. See specific guidelines for children below.
- Staff shall ensure that all personal information is kept securely.
- Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party. *Unauthorised disclosure may be a disciplinary matter, and may be considered gross misconduct in some cases.*

Employees can request access to the information held on them by the Company. All requests by employees to gain access to their personnel records should be made in writing.

Sensitive Information

- The Rushmere Academy may process sensitive information about a person's health, disabilities, criminal convictions, race or ethnic origin, or trade union membership. For example, some contracts or courses will bring the applicants into contact with children, including young people between the ages

of 12-18, and The Rushmere Academy has a duty under the Children Act 1989 and other enactment to ensure that staff are suitable for the job, and students for the courses offered.

- The Rushmere Academy also asks for information about particular health needs, such as allergies to particular forms of medication, or conditions such as asthma or diabetes. The Rushmere Academy will only use such information to protect the health and safety of the individual, for example, in the event of a medical emergency.

Retention of Data

The Rushmere Academy will keep different types of information for differing lengths of time, depending on legal, academic and operational requirements. Information and advice about the recommended retention times are available.

Compliance

Compliance with the Act is the responsibility of all students and members of staff. Any deliberate or reckless breach of this Policy may lead to disciplinary, and where appropriate, legal proceedings.

Any individual, who consider that the policy has not been followed in respect of personal data about him or herself, should raise the matter with one of the Directors initially. If the matter is not resolved it should be referred to the staff grievance or student complaints procedure.

Specific Guidance for controlling and processing data relating to children.

Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.

If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.

Compliance with the data protection principles and in particular fairness should be central to all your processing of children's personal data.

You need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.

If you are relying on consent as your lawful basis for processing, when offering an online service directly to a child, in the UK only children aged 13 or over are able to provide their own consent.

For children under this age you need to get consent from whoever holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service.

Children merit specific protection when you use their personal data for marketing purposes or creating personality or user profiles.

You should not usually make decisions based solely on automated processing about children if this will have a legal or similarly significant effect on them.

You should write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have.

Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.

An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

Checklists

- Bases for processing a child's personal data
- When relying on consent, we make sure that the child understands what they are consenting to, and we do not exploit any imbalance of power in the relationship between us.
- When relying on 'necessary for the performance of a contract', we consider the child's competence to understand what they are agreeing to, and to enter into a contract.
- When relying upon 'legitimate interests', we take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.
- Protect the personal data you hold.
- An ICO certificate is in date and held.

For computer security:

- Install a firewall and virus checking on computers
- Make sure that your operating system is set up to receive automatic updates
- Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.
- Only allow staff access to the information they need to do their job.
- Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.
- Take regular back-ups of the information on your computer system and keep them in a separate place so that if computers are lost the information would not be lost.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).

- Consider installing an anti-spyware tool. Spyware is the generic name given to programs that are designed to monitor activities on computers. Spyware can be unwittingly installed within other file and program downloads, their use is often malicious. It can capture passwords, banking credentials and credit card details which can be relayed fraudulently. Anti-spyware helps to monitor and protect computers from spyware threats.

For using emails securely:

- Consider whether the content of the email should be encrypted or password protected.
- Ensure correct email address is used when auto-complete suggests recipients.
- Use bcc (blind carbon copy) function to send email to additional recipients without revealing their information.
- When sending a group email ensure message is definitely meant for all members of group.
- If a sensitive email is sent from a secure server to an insecure recipient, security will be threatened. Check recipients email is secure before sending messages.

For other security:

- Shred all confidential paper waste
- Check physical security of premises.
- Use a strong password – at least seven characters with a combination of upper and lower case letters and numbers.
- Do not open spam mail
- Never give out passwords

References.

For any further guidance on The Data Protection Act 2018 and the GDPR reference should be made to https://ico.org.uk. The website contains a wealth of help, guidance and best practice for compliance.