DATA PROTECTION & GDPR POLICY

Policy control table			
Policy title:		Data Protection & GDPR Policy	
Author:		David Thorpe	
Policy Version:		3	
Approved on:			
Approved by:			
Review Date:		July 2025	
Document History			
Version	**Date**	**Author**	**Note of revisions**
3	July 2024	David Thorpe	Last reviewed July 2024

Contents

Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format

Data Protection Policy Statement

The school is committed to a policy of protecting the rights and privacy of individuals (includes students, staff and others) in accordance with the Data Protection Act. The School needs to process certain information about its staff, students and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programmes of study, to record progress, to collect fees, and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The policy applies to all staff and students of Rotherham Aspire. Any breach of the Data Protection Act 1998 or the School Data Protection Policy is considered to be an offence and, in that event, Rotherham Aspire disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with Rotherham Aspire, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that departments/sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

Sensitive Data

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual orientation, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

Data Controller

Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the Data Subject Any living individual who is the subject of personal data held by an organisation.

Rotherham Aspire must comply with data protection legislation and is the responsibility of all members of the organisation who process personal information Members of the company are responsible for ensuring that any personal data supplied to the company is accurate and up-to-date.

- Data protection principles state that processing of personal data must be done in accordance with the eight data protection principles:
- Personal data shall be processed fairly and lawfully. Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

- Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes. Data obtained for specified purposes must not be used for a purpose that differs from those.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held. Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed.
- Personal data shall be accurate and, where necessary, kept up to date. Data, kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume accurate. It is the responsibility of individuals to ensure that data held by Rotherham Aspire is accurate and up-to-date. Completion of an appropriate registration or application form will be taken, as an indication that the data contained therein is accurate. Individuals should notify Rotherham Aspire of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Rotherham Aspire to ensure that any notification regarding change of circumstances is noted and acted upon.
- Personal data shall be kept only for as long as necessary.
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.
- Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Data must not be transferred outside of the European Economic Area (EEA) - the EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual.

Members of Rotherham Aspire should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. Rotherham Aspire understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual
- The data needs to be processed so that the school can comply with a legal obligation The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent
- For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018

Security of Data

All staff are responsible for ensuring that any personal data (on others), which they hold, are kept securely and that they are not disclosed to any unauthorised third party. All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- In a lockable room with controlled access.
- In a locked drawer or filing cabinet.
- If computerised, password protected.
- Kept on disks which are themselves kept securely.
- PCs and terminals not visible except to authorised staff
- Computer passwords are kept confidential.
- Manual records not be left where they can be accessed by unauthorised personnel.
- Appropriate security measures are in place for the deletion or disposal of personal data.
- Manual records be shredded or disposed of as "confidential waste".
- Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff and students who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and students should take particular care when processing personal data at home or in other locations outside the Training Centre. Rights of Access to Data Members of the Training Rotherham Aspire have the right to access any personal data, which are held by Rotherham Aspire in electronic format and manual

records, which form part of a relevant filing system. This includes the right to Rotherham Aspires confidential personal references received by Rotherham Aspire about that person.

Any individual who wishes to exercise this right should apply in writing to the Data Protection Officer. Rotherham Aspire reserves the right to charge a fee for data subject access requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee. In order to respond efficiently to subject access requests Rotherham Aspire needs to have in place appropriate records management practices.

Disclosure of Data: Rotherham Aspire must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and students should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible.

Subject access requests and other rights of individuals

Subject access requests Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual

Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual Subject access requests must be submitted in writing, either by letter or email to the school or the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the School Business Manager or the DPO.

Children and subject access requests:

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by- case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

Legal Framework

1 This policy has due regard to legislation, including, but not limited to the following:
- The General Data Protection Regulation(GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of information and Data Protection (Appropriate Limit and Fees) regulations 2004
- The Schools Standards and Framework Act 1998

2 This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) "Overview of the General Data Protection Regulation(GDPR)"

- Information Commissioners' Office (2017) Preparing for the General Data Protection regulation(GDPR) 12 steps to take now"

3 This policy will be implemented in conjunction with the following other school policies:

- Photography and videos at school Policy
- E-Security Policy
- Freedom of Information Policy
- CCTV Policy