Data Protection Policy

Updated: March 2022
Produced by: Mrs E Swansbury
School Business Manager
Ratified by: To be ratified by the Board of Trustees

Signed:

Chair of Trustees Headteacher

Review Date: February 2024

This page has been intentionally left blank

Contents

1. Introduction

1.1. Ryhope Infant School Academy's Data Protection Policy has been produced to ensure compliance with the Data Protection Act 2018 (DPA), which is the UK's implementation of the General Data Protection Regulation (GDPR) and associated legislation, alongside guidance from the Information Commissioner's Office (ICO).

1.2. The DPA gives individuals rights over their personal data and protects the use of personal data.

1.3. Ryhope Infant School Academy is registered with the ICO as a Data Controller for the processing personal information.

2. Purpose

2.1. Ryhope Infant School Academy Data Protection Policy has been produced to ensure its compliance with the DPA 2018.

2.2. The Policy incorporates guidance from the ICO, and outlines the Academy's approach to its responsibilities and individuals' rights under the DPA 2018.

3. Scope

3.1. This Policy applies to all employees (including temporary, casual or agency staff and contractors, consultants and suppliers working for, or on behalf of, the Academy), third parties and others who may process personal information on behalf of the Academy.

3.2. The Policy also covers any staff and students who may be involved in research or other activity that requires them to process or have access to personal data, for instance as part of a research project or as part of professional practice activities. If this occurs, it is the responsibility of the Academy to ensure the data is processed in accordance with the DPA 1998 and that students and staff are advised about their responsibilities.

4. Data covered by the Policy

4.1. In summary, personal data is information relating to a living individual where the structure of the data allows the information to be accessed i.e. as part of a relevant filing system. This includes data which allows an individual to be identified when put together with other information held by the Academy. Data is covered where it is held manually or electronically and data compiled, stored or otherwise processed by the Academy, or by a third party on its behalf.

4.2. Special category personal data is personal data consisting of information relating to:

4.3. Racial or ethnic origin

4.4. Political opinions,

4.5. Religious or philosophical beliefs

4.6. Membership of a trade union

4.7. Physical or mental health or condition

4.8. Sexual life or sexual orientation

4.9. Commission or alleged commission of any offence

4.10. Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

5. The Six Data Protection Principles

5.1. The DPA 2018 requires the Academy, its staff, and other organisations who process personal information on behalf of the Academy, to comply with the six data protection principles.

5.2. The principles require that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- Be adequate, relevant and not excessive for those purposes
- Be accurate and kept up to date
- Not be kept for longer than is necessary for those purpose
- Be kept safe from unauthorised or unlawful processing and against accidental loss, destruction or damage

5.3. As the controller we shall be responsible for and be able to demonstrate compliance with, the above six principles.

6. Responsibilities

6.1. The Academy has a designated Data Protection Officer (DPO) to support and advise on day-to-day issues which arise, and to provide members of the Academy with guidance on Data Protection issues to ensure they are aware of their obligations.

6.2. The Head Teacher and School Business Manager acts as representatives of the data controller on a day-to-day basis.

6.3. All new members of staff will be required to undertake mandatory Data Protection training as part of their induction, and existing staff will be requested to undertake refresher training on a regular basis.

6.4. Employees of the Academy are expected to:

6.5. Familiarise themselves and comply with the six data protection principles

6.6. Ensure any processing of personal data is accurate and up to date

6.7. Ensure their own personal information is accurate and up to date

6.8. Keep personal data for no longer than is necessary

6.9. Ensure that any personal data they process is secure and in compliance with the Academy's information related policies and strategies

6.10. Acknowledge data subjects' rights (e.g. right of access to all their personal data held by the Academy) under the DPA 2018, and comply with requests to exercise those rights

6.11. Ensure personal data is only used for those specified purposes and is not unlawfully used for any other business that does not concern the Academy

6.12. Obtain consent where necessary to collect, share or disclose personal data

6.13. Contact the School Business Manager or the DPO for advice if they have concerns or are in doubt about data protection requirements to avoid any infringements of the DPA 2018.

6.14. Students of the Academy are expected to:

- Comply with the six data protection principles
- Comply with any security procedures implemented by the Academy.

7. Obtaining, Disclosing and Sharing

7.1. Only personal data that is necessary for a specific reason related to the provision of education or employment by the Academy should be obtained. Under DPA, there are six lawful bases for processing personal information:

- The data needs to be processed so that the Academy can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract (e.g. employment)
- The data needs to be processed so that the Trust can **comply with a legal obligation** (e.g. Education Act 2011, Children's Act 2004)
- The data needs to be processed to ensure the **vital interests** of the individual (e.g. to protect someone's life)
- The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest,** and carry out its official functions (e.g. deliver education)
- The data needs to be processed for the **legitimate interests** of the Academy 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** (e.g. school trips, photos)

7.2. For special categories of personal data, as identified in section 4, the Academy will also meet one of the special category conditions for processing which are set out in the Data Protection Act 2018.

7.3. Students and staff are informed about how their data will be processed via the Academy's Privacy Notices.

7.4. Upon acceptance of employment at the Academy, members of staff also agree to the processing and storage of their data.

7.5. Data must be collected and stored in a secure manner.

7.6. Personal information will not be disclosed to a third-party organisation without the prior consent of the individual concerned unless required by law (see 7.6 below). This also includes information that would confirm whether or not an individual is or has been an applicant, student or employee of the Academy.

7.7. The Academy may have a duty to disclose personal information in order to comply with a legal or statutory obligation. The DPA 2018 allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function. Any requests to disclose personal data for reasons relating to national security, crime and taxation should be directed to the DPO at Data.Protection@sunderland.gov.uk.

7.8. Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the purview and boundaries of sharing. For circumstances where personal information would need to be shared in the case of ad hoc arrangements, sharing shall be undertaken in compliance with the DPA 2018.

7.9. Where a third-party processes information on behalf of the Academy, the Academy will only use organisations that provide sufficient guarantees that they have technical and organisational measure in place to safeguard the information. All such processing will be governed by a contract.

8. Retention, Security and Disposal

8.1. Recipients responsible for the processing and management of personal data need to ensure that the data is accurate and up-to-date. If an employee, student or applicant is dissatisfied with the accuracy of their personal data, then they should inform the School Business Manager or the Academy's DPO.

8.2. Personal information held in paper and electronic format shall not be retained for longer than is necessary. In accordance with principle 2 and principle 4 of the DPA 2018, personal information shall be collected and retained only for business, regulatory or legal purposes.

8.3. In accordance with the provisions of the DPA 2018, all staff whose work involves processing personal data, whether in electronic or paper format, must take responsibility for its secure storage and ensure appropriate measures are in place to prevent accidental loss or destruction of, or damage to, personal data.

8.4. In accordance with the Academy's Flexible Working Scheme, staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others.

8.5. All departments should ensure that data is destroyed in accordance with the Retention Schedule when it is no longer required.

8.6. Personal data in paper format must be shredded or placed in the confidential waste bins provided. Personal data in electronic format should be deleted, and CDs and pen drives that hold personal data passed to our I.T provider for safe disposal. Hardware should be appropriately rendered redundant and disposed of in compliance with our I.T service provider contract and to ensure it conforms with DPA and GDPR requirements.

9. Transferring Personal Data

9.1. Any transfer of personal data must be carried out securely in line with the framework provided by the following:

- Data Protection Act 2018 and GDPR
- Caldicott: To Share or not to Share – The Information Governance Review 2013
- The ICO Code of Practice on Data Sharing 2015
- Information Sharing Advice for Safeguarding Practitioners 2015.

9.2. Email communications should be assessed for risks to individuals' privacy. Wherever possible, sending personal data via encrypted email should be the preferred transit medium, with a password provided to the recipient by a separate medium.

9.3. Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important that emails are addressed correctly and care is taken when using reply all or forwarding or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

9.4. Personal email accounts should not be used to send or receive personal data for work purposes.

10. Data Subjects Right of Access (Subject Access Requests)

10.1. Under the DPA 2018, individuals (including staff and students) have the right to request access to their personal data held by the Academy. This applies to data held in both paper and electronic format, and within a relevant filing system.

10.2. The Academy may, with the advice of the DPO, use its discretion under the DPA 2018 to encourage informal access at a local level to a data subject's personal information, but it will also have a formal procedure for the processing of Subject Access Requests.

10.3. Any individual who wishes to exercise this right should make the request in writing or via the submission of a Subject Access Request Form.

10.4. 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.

10.5. Children below the age of 12 are generally not 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 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.

10.6. The Academy may not charge a fee. It will only release any information upon receipt of a valid request, along with proof of identity, or proof of authorisation where requests are made on the behalf of a data subject by a third party. The requested information, or reason for refusing a request, will be provided within the statutory timescale of **1 calendar month** from receipt of a valid request.

11. Reporting a Data Security Breach

11.1. It is important the Academy responds to a data security breach quickly and effectively. A breach may arise from a theft, a deliberate attack on Academy systems, unauthorised use of personal data, accidental loss or equipment failure. Any data breach should be reported to the School Business manager in the first instance who will also inform the DPO at **Data.Protection@sunderland.gov.uk.** If the breach relates to an IT incident (including information security), it should also be reported to the Head Teacher and in certain circumstances to our I.T provider. Please refer to the Data Breach Report Form for more information.

11.2. Any breach will be investigated in line with the procedures within the Data Breach Report Form (appendix 1.). In accordance with that procedure, the Academy will treat any breach as a serious issue. Each incident will be investigated and judged on its individual circumstances and addressed accordingly.

12. Policy retention and review

12.1. This policy will be reviewed biennially or sooner if there is a change in legislation.

12.2. A copy of the policy in place from time to time will be retained until the end of the period of 6 months beginning on the day processing under that version of the policy ceases.

Appendix 1: Data Breach Report Form

What is a data breach? A data breach is whenever the confidentiality, integrity and availability of information is compromised. Data doesn't only need to be stolen to be breached through instances of cyber-crime; it might also have been lost, altered, corrupted or accidentally disclosed.

Please act promptly to report a data breach. If you discover a data breach please notify the School Business manager or the Head Teacher immediately.

SECTION 1: Notification of data security breach (to be completed by the person reporting the incident)

Date of the incident:	
Date incident was discovered:	
When was the SBM/Headteacher notified of the breach:	
Place of the incident:	
Contact details of person reporting incident (email and telephone):	
Brief description of incident. **Consider to following when responding:** • What data was involved? • What happened to the data, has it been lost, altered, corrupted or accidentally disclosed? • How did the breach happen?	
Number of Data Subjects (individuals) affected, if known	
Has any personal data been placed at risk? If so, please provide details:	
Brief description of any action taken at the time of the discovery:	
For use by the School Business Manager or Head Teacher:	
Received by:	
Date Received:	
Forwarded for action to:	
Date forwarded for action:	

SECTION 2: Assessment of severity (to be completed by the School Business Manager (SBM) in consultation with the Head Teacher and IT Manager, where appropriate)

Details of the IT systems, equipment, devices, and records involved in the security breach:	
Details of the information loss/breach:	
What is the nature of the information lost?	
What protection was in place? i.e. encryption	
How much data has been lost? If a laptop is lost or stolen, how recently was this last backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, legal, liability, or reputational consequences for the Academy or third parties?	
How many Data Subjects are affected?	
What are the potential effects on those data subjects?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into the following categories:	
HIGH RISK personal data. Special Category data (as defined in the Data Protection Act 2018) relating to a living, identifiable individual's: a) Racial or ethnic origin; b) Political opinions or religious or philosophical beliefs; c) Membership of a trade union; d) Physical or mental health, or condition, or sexual life; e) Biometric data	
Information that could be used to commit identity fraud such as: a) Personal bank account and other financial information; b) National identifiers, such as NI number; c) Copies of passports or visas	
Personal information relating to parents, staff and children	
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant	

damage or distress to that person if disclosed	
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline, or sensitive negotiations which could adversely affect individuals	
Security information that would compromise the safety of individuals if disclosed	
What actions have been taken?	
Has the initial incident been contained? When? How?	
Have existing controls been reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring? **Consider:** • Where and how the personal data is held and where it is stored; • Where the biggest risks lie, and will identify any further potential weak points within its existing measures; • Whether methods of transmission are secure - sharing the minimum amount of data necessary • Identifying weak points within existing security measures; • Staff awareness; • Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security	
Has a full review of the causes of the breach, the effectiveness of the response and whether any changes to systems, policies or procedures been undertaken?	
Are there any wider consequences to the breach	

SECTION 3: Action taken: (to be completed by the Data Protection Officer and / or School Business Manager (SBM) in consultation with the Head Teacher, where appropriate)

Incident number (e.g. year/001):	
Report received by:	
Date report received:	
Action taken by responsible officers:	
Was incident reported to the police (YES/NO)? If notified please record the date:	
Follow up action required or recommended:	

SECTION 4: Notifications (to be completed by the Data Protection Officer and / or School Business Manager (SBM) in consultation with the Head Teacher, where appropriate)

As part of the investigation, the SBM/HT and/or DPO must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

The SBM/HT and/or DPO should also consider whether any press release may be required.

All actions **MUST** be recorded by the SBM/HT and/or DPO.

For use by the Data Protection Officer, Head Teacher or School Business Manager

Notification to the ICO within 72 hours of being notified of the breach (YES/NO). If yes, please record detail of notification and date notified:	
Notification to Data Subjects (YES/NO). If yes, please record detail of notification and date notified:	
Notification to other external regulator or stakeholder (YES/NO). If yes, please record detail of notification and date notified:	

Appendix 2: Subject Access Request Form

PERSONAL DETAILS

We need your personal details to find the personal data that we hold about you and your child.

We will keep this form on file for up to two years after we reply to your request. We may transfer some of the information you provide to a computerised database to help us monitor and improve our performance. After two years we will destroy this form and delete identifying details from our database.

Your Name	
Your date of birth **(Only if requesting your data)**	
Child/Children's Name/s	
Date of birth of your child/children **(Only if requesting their data)**	
Only people who have parental responsibility or the child themselves if over, the age of 13 can access data about them	
Please confirm your relationship to the child	
Current address and postcode	
Telephone number	
If you have lived at this address for less than two years please provide your previous address and postcode	
Please provide any additional information you think we may need to find your personal data i.e. the dates you/your child attended our school, if not a current pupil	

Data Subject Declaration

I wish to access personal data that Ryhope Infant School Academy holds. I understand that the Academy will need to confirm my identity and my relationship to the child, if I am making a request to access a child's data. I understand that the Academy may need to contact me to obtain more information from me to find the data that I have requested.

The 30-day reply period begins once I have provided all the information the Academy needs.

Please send me all of the information I am entitled to under the Data Protection Act 2018

Signed:

Date:

Agent's Declaration

If you are **NOT** the data subject but have authority to act on his or her behalf, you must complete this declaration.

I understand that Ryhope Infant School Academy may need to contact me to confirm my identity. I understand that the Academy may need more information from me to find the personal data that I have requested.

The 30-day reply period begins once I have provided all the information the Academy needs.

I confirm that I act on behalf of the Data Subject named overleaf and I have shown to the Academy proof of my authority to do so.

Signed:

Date:

Please return this form to:

Ryhope Infant School Academy

Shaftesbury Avenue

Sunderland

SR2 0RT

Email: info@ryhopeinfantschool.org.uk

Tel: 0191 9171910