DATA PROTECTION POLICY

This policy applies to all academies within Bonitas Multi-Academy Trust

Date last reviewed	Spring 2025
Review period	Every 2 years
Date of next review	Summer 2027
Owner	CEO / Head of IT
Approved by	Board of Trustees
Date approved	June 2025
Associated documents/information	• Whistle-Blowing Policy • Data Retention Policy • Complaints Policy

Data Protection Policy

1. Introduction

This Data Protection Policy outlines how the Bonitas Multi-Academy Trust (the "Trust", “we”, “us”) its academies, and its central services team handle personal data to ensure compliance with the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR). The Trust is committed to processing personal data fairly, lawfully, and securely.

As a Data Controller, the Trust acknowledges its responsibility under the DPA 2018 and will take all reasonable steps to meet this responsibility, promoting good practice in the handling and use of personal information in accordance with this Policy.

It is the responsibility of the Local Governing Body (LGB) and Headteacher of each school, as well as the Board of Trustees (the Board) and the Chief Executive Officer (CEO) for Trust central services, to ensure that their school or service and its staff understand and adhere to this Policy. In implementing this Policy, the LGB, Headteacher, and Trust staff must take account of any advice provided by the CEO and/or the Board.

This Policy is subject to the Scheme of Delegation approved for the Trust and its schools or services. In the event of any ambiguity or conflict, the Scheme of Delegation (the Scheme) and any specific amendments or restrictions approved by the Board will take precedence. If there is any uncertainty regarding the interpretation or implementation of this Policy, the CEO should be consulted.

2. Scope

This policy, along with any associated policies, applies to all employees, trustees, governors, students, parents, suppliers, and any other individuals who interact with the Trust and its academies. It covers all personal data processed by the Trust, whether stored in electronic or paper format.

3. Legal Framework

The Trust is committed to complying with the following legal requirements:

- The Data Protection Act 2018
- UK General Data Protection Regulation
- Freedom of Information Act 2000
- Education Act 1996
- Protection of Freedoms Act 2012

4. Data Protection Principles

The Trust adheres to the principles set out in the UK GDPR, ensuring that personal data is:

- processed lawfully, fairly, and in a transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

- accurate and, where necessary, kept up to date
- kept for no longer than necessary for the purposes for which it is processed
- processed in a way that ensures it is appropriately secure, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

The Trust and its schools will:

- apply records management policies and procedures to ensure that information is not held longer than necessary
- ensure that when information is authorised for disposal, it is done appropriately
- ensure appropriate security measures are in place to safeguard personal information, whether held in paper files or on a computer system
- only share personal information with others when necessary and legally appropriate to do so
- set out clear procedures for responding to requests for access to personal information (known as subject access in the Data Protection Act)
- train all staff to ensure they are aware of their responsibilities and of the Trust's relevant policies and procedures

5. Definitions

The Trust, its schools and individuals will have access to a wide range of personal data which may be held in either digital format or paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their family or their circumstances:

Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: › Name (including initials) › Address › Identification number › Contact details › Curricular/academic data e.g. class lists, pupil/student progress reports, reports, references › Professional records e.g. employment history, taxation and national insurance records, appraisal records and references › Factors specific to an individual's physical, genetic, physiological, mental, economic, cultural or social identity › Other information that might be disclosed by parents/carers or other agencies working with families or staff members.

Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: › Racial or ethnic origin › Political opinions › Religious or philosophical beliefs › Trade union membership › Genetics › Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes › Health – physical or mental › Sex life or sexual orientation
Processing	Anything done to personal data, ie. collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

6. Roles and Responsibilities

This policy applies to all staff employed by the Trust and its schools, including volunteers, and to external organisations or individuals working on behalf of the Trust and its schools. Staff, who fail to comply with this policy may face disciplinary action.

6.1 The Data Controller

The Trust processes personal data relating to parents, pupils, staff, Trustees, Governors, Members, visitors and others, and is therefore a data controller. As such, the Trust is registered with the Information Commissioner's Office (ICO) as a data controller and will renew this registration annually or as otherwise legally required.

6.2 The Trustees

The Trustees have overall responsibility for ensuring that the Trust meets all relevant data protection obligations.

6.3 Data Protection Officer

The Trust and its schools are supported in fulfilling their data protection responsibilities by an externally appointed Data Protection Officer (DPO) who serves as the first point of contact for the ICO. The name and contact details of the DPO for the Trust are provided in Appendix 1.

The Trust appointed lead for data protection is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. They report directly to the Board of Trustees, operate independently and cannot be dismissed or penalised for performing their duties. They will provide an annual report of Trust activities to the Board and, where relevant, offer their advice and recommendations on trust data protection issues. The name and contact details of the appointed lead is provided in Appendix 1.

Each school within the Trust has a designated member of the Senior Leadership Team (SLT) responsible for overseeing the implementation of this policy, ensuring compliance with data protection law, and developing related guidelines where applicable. The designated SLT member is the first point of contact for individuals whose data the school processes. They report to the LGB, operate independently and cannot be dismissed or penalised for performing their duties. They will provide an annual report of their activities to the Trust appointed lead and, where relevant, report their advice and recommendations on school data protection issues. The name and contact details of the designated member of the SLT in each school are provided in Appendix 1.

6.4 CEO / Headteacher

The CEO and Headteachers act as the representative of the data controller on a day-to-day basis and ensure that data protection measures are embedded in daily operations.

6.5 Information Asset Owners

The Trust will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil/student information/staff records/assessment data). The IAOs will be responsible managing and addressing risks associated with holding the information and will understand:

- The data they are responsible for – including its purpose, sensitivity, and how it is collected, stored, and shared.
- Potential risks and threats – identifying vulnerabilities and implementing measures to protect the data from unauthorised access, loss, or breaches.
- Legal and regulatory requirements – ensuring compliance with data protection laws, such as GDPR, and any Trust policies related to data security and privacy.
- Data access and sharing protocols – controlling who can access the information and ensuring that any sharing of data is done securely and appropriately.
- Retention and disposal policies – managing data throughout its lifecycle and ensuring it is securely deleted or archived when no longer needed.
- Incident response responsibilities – knowing the procedures for reporting and responding to data breaches or security incidents.

6.6 All staff

All Members, Trustees, Governors, staff, contractors and volunteers are responsible for:

- Collecting, storing and processing any personal data in accordance with this Policy
- Informing the Trust of any changes to their personal data, such as a change of address

In circumstances where staff have questions or concerns relating to data protection, they should contact the member of SLT with oversight of data protection. Alternatively, they may contact the DPO direct using the details provided in Appendix 1.

Queries and concerns may include the following circumstances:

- questions about the operation of this Policy, data protection law, retaining personal data or keeping personal data secure
- that this Policy is not being followed
- they are unsure whether or not they have a lawful basis to use personal data in a particular way
- they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area (EEA)
- there has been a data breach
- they are engaging in a new activity that may affect the privacy rights of individuals
- they need help with any contracts or sharing personal data with third parties.

7. Collecting and using Information

7.1 Lawfulness, fairness and transparency

The Trust ensures that any processing of personal data is justified under one of the six 'lawful bases' (legal reasons) and is carried out in compliance with data protection laws. These are:

- **Consent** – The individual has given clear and explicit permission for their data to be processed for a specific purpose.
- **Contract** – Processing is necessary to fulfill a contract with the individual or to take steps at their request before entering into a contract.
- **Legal Obligation** – Processing is required to comply with a legal obligation.
- **Vital Interests** – Processing is necessary to protect someone's life or prevent serious harm.
- **Public Task** – Processing is required to carry out a task in the public interest or in the exercise of official authority.
- **Legitimate Interests** – Processing is necessary for the legitimate interests of the Trust or a third party, provided these interests are not overridden by the rights and freedoms of the individual.

For special categories of personal data, the Trust will ensure that processing is justified under one of the special category conditions set out in the GDPR and the DPA 2018. These conditions provide additional safeguards due to the sensitive nature of the data, such as information relating to health, ethnicity, religious beliefs, or biometric data. The Trust is committed to handling special category data lawfully, fairly, and transparently, ensuring appropriate safeguards are in place to protect individuals' rights and privacy.

7.2 Limitation, minimisation and accuracy

The Trust will collect personal data only for specified, explicit and legitimate purpose. These purposes will be explained to individuals at the time their data is first collected.

If the Trust intends to use personal data for reasons other than those originally stated it will inform the individuals concerned beforehand and seek consent where necessary.

Staff must process personal data only when it is necessary for carrying out their job responsibilities.

The Trust is committed to maintaining accurate and up-to-date data. Any inaccurate information will be corrected or erased as appropriate. When personal data is no longer needed, staff must ensure it is securely deleted or anonymised in accordance with the Trust's record retention schedule.

7.3 Information to stakeholders "Privacy Notices"

To comply with the fair processing requirements of the DP Act 2018, the Trust is committed to informing all stakeholders, including staff, pupils, parents/carers, and those who govern, about the data it collects, processes, and holds. This includes the purpose for which data is held and the third parties with whom it may be shared (e.g. Local Authority, DfE.

Privacy notices will be made available to parents/carers via the Trust and schools' websites. These notices will also be provided to staff, pupils, and governors where applicable, ensuring that all individuals involved are aware of how their data is processed. Any updates to these notices will be communicated through email and/or a letter home, as appropriate.

For parents/carers of pupils/students joining the Trust, a link to the privacy notice will be included in the information pack and registration form provided during the enrollment process. Similarly, for staff, governors, and pupils, the relevant privacy notices will be shared at the start of their engagement with the Trust, ensuring they understand how their personal data will be handled.

8. Secure storage and access to information

8.1 The Trust will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure. It will also safeguard data against accidental or unlawful loss, destruction, or damage. Data will be protected throughout its whole lifecycle, from creation to deletion. This covers data in use, in transit, and in rest across all forms of media, electronic or otherwise.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives containing personal data, must be securely stored under lock and key when not in use.
- Confidential personal data should never be left on office or classroom desks, staffroom tables, or display boards. The Trust will follow a "Clear Desk" approach to protect data.
- Visitors must not be left unattended with Trust data, and care should be taken to ensure no Trust data is visible in offices or meeting rooms.
- Off-site personal data—for example, data taken on school trips—must be signed in and out at the school office, and staff must take all reasonable steps to protect the information.

- Strong passwords are required for all users. Passwords must never be shared and should differ from those used for personal accounts (e.g., Gmail, LinkedIn).
- Password-protected devices are necessary for accessing personal data. Any device accessing data must be locked if left unattended (even for short periods) and set to auto-lock after 10 minutes of inactivity.
- Data sharing should be done via Trust-provided tools such as OneDrive or SharePoint. When sharing documents, send a link rather than attaching personal data to an email. Do not use external sites (e.g., Dropbox, personal Google Drive) for sharing or storing Trust data.
- Personal devices used for accessing Trust data must be secured with a password, PIN, or equivalent. Mobile devices should also be configured to allow remote data wiping in case of theft.
- Access to Trust services on personal devices must require a password whenever accessing services like Trust email. Services should not remain logged in.
- Personal data should only be stored on Trust equipment. Private equipment (e.g., personal laptops or phones) must not be used for storing Trust data.
- Data sharing outside the Trust must be done only after verifying the recipient's identity and ensuring there is a legal basis for sharing the data. Data can only be shared with external parties that have signed an appropriate data-sharing or confidentiality agreement.
- Telephone or Internet surveys must not be participated in without prior authorisation from the Trust.
- Suspicious third-party interactions or incidents that may negatively impact the Trust's integrity or reputation must be reported to the DPO.
- Public discussions of personal, confidential, or privileged information should be avoided to protect the integrity and confidentiality of the data.

8.2 The Trust will ensure that systems are set up to hide the existence of protected files from unauthorised users. Users will be assigned clearance that will determine the files they can access. Access to protected data will be controlled according to the role of the user within the Trust. Members of staff will not, as a matter of course, be granted access to the whole management information system.

8.3 When personal data is stored on any laptop, other portable computer system, USB stick or other removable media:

- the data must be encrypted and password protected;
- the device must be password protected;
- where possible, the device must offer approved virus and malware checking software; and
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

8.4 The Trust has clear policies and procedures in place for the automatic back up, access and restoration of all data held on school systems, including off-site backups. See Appendix 5.

8.5 The Trust has clear policies and procedures for the use of "Cloud Based Storage Systems". The Trust is aware that data held in remote and cloud storage must still be protected in line with the DPA 2018. The Trust will ensure that it is satisfied with the controls put in place by remote/cloud-based data services providers to protect this data.

8.6 Access out of school

The Trust recognises that personal data may be accessed by teachers and other users out of school. In these circumstances:

- Users may not remove or copy sensitive, restricted or protected personal data from the Trust, its schools or authorised premises without permission. Any media used must be encrypted and password protected, and transported securely for storage in a secure location
- Users must take particular care that computers or removable devices containing personal data are not accessed by unauthorised users (e.g. family members) when off school premises
- When restricted or protected personal data is required by an authorised user outside of the Trust's premises (e.g. a member of staff working from home), secure remote access to the management information system or learning platform is preferred.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data if the storage media, or portable device is encrypted and is transported securely for storage in a secure location;
- All portable and mobile devices, including media, used to store or transmit personal information, must be protected with approved encryption software;
- Particular care should be taken if data is taken or transferred to another country, particularly outside of Europe.

9. Sharing data

9.1 The Trust may share personal data with third parties such as:

- Local authorities
- The Department for Education (DfE)
- Exam boards

The Trust will not normally share personal data without consent but may be required to do so in the following circumstances:

- Safety concerns: When there is an issue involving a pupil, student, or parent/carer that puts the safety of staff at risk.
- Liaising with other agencies: The Trust will seek consent where necessary before sharing personal data with external agencies.
- Engaging suppliers or contractors: If suppliers or contractors require access to personal data to provide services to staff and students (e.g., IT companies), the Trust will:
    - Only appoint suppliers or contractors that can demonstrate compliance with data protection law.
    - Establish a data-sharing agreement in the contract or as a standalone agreement to ensure fair and lawful processing of shared data.
    - Share only the minimum necessary data required for the supplier or contractor to perform their service, including information needed to keep them safe while working with the Trust and its schools.

The Trust will also share personal data with law enforcement and government bodies where legally required to do so, including for:

- Preventing or detecting crime and fraud

- Apprehending or prosecuting offenders
- Assessing or collecting tax owed to HMRC
- Complying with legal proceedings
- Fulfilling safeguarding obligations
- Supporting research and statistical analysis, provided that personal data is sufficiently anonymised or consent has been obtained

9.2 The Trust may share personal data with emergency services and local authorities to help them to respond to an emergency situation affecting pupils or staff.

9.3 If the Trust transfers personal data to a country or territory outside the EEA, it will do so in accordance with data protection law.

10. Subject access requests (SARs)

The Trust recognises that under Article 15 of the UK GDPR and the DPA 2018, data subjects have the right to access their personal data. The Trust has established procedures, as set out in Appendix 3, to ensure that all SARs are handled in compliance with current legislation, including the requirement to respond within one month of receipt of the request (or within an extended period of up to two additional months in complex cases, with notification to the requester).

Further information about data subject rights and how to exercise them is available from the Information Commissioner's Office (ICO): https://ico.org.uk

Individuals have a right to make a Subject Access Request (SAR) to access personal information held by the Trust. This includes:

- Confirmation of whether their personal data is being processed
- Access to a copy of their personal data
- The purposes of data processing
- The categories of personal data concerned
- Details of who the data has been, or will be, shared with
- How long the data will be stored for, or if not possible, the criteria used to determine this period
- Where applicable, the right to request rectification, erasure or restriction, or to object to processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not provided by the individual
- Whether any automated decision-making is being applied to their data, and what significance and/or consequence this might have for the individual
- The safeguards in place if the data is being transferred internationally

SARs can be submitted in any form, but the Trust may process requests more efficiently if they are made in writing and include:

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

Individuals should submit SARs to the Headteacher or the (DPO). They may also inform the senior leader responsible for data protection within the Trust or individual school. If any Trust staff member receives a SAR, they must immediately forward it to the CEO or designated DPO for action. See Appendix 4.

10.1 Additional Data Rights

Individuals also have the right to:

- Withdraw their consent to processing at any time
- Prevent the use of their personal data for direct marketing
- Challenge processing based on public interest grounds
- Request copies of agreements related to international data transfers (outside of EEA)
- Prevent processing that is likely to cause damage or distress
- Request the transfer of their personal data to a third party in a structured, commonly used, and machine-readable format (where applicable)

10.2 Children and general information and / or subject access requests

A child's personal data belongs to the child, not their parents or carers. Parents or carers may only make a SAR or general information request on behalf of the child if the child lacks the maturity to understand their data rights and the implications of the request, or if the child has explicitly consented to the request.

A child can also make a general information request about their data, and the same principles apply as for a SAR. Parents or carers may assist or make the request on behalf of the child in certain circumstances, particularly where the child is under 13 years of age.

A child may not be considered mature enough to make their own decision if they do not fully understand what they are asking for or if their request could cause them harm. In these cases, the school must decide what is in the child's best interests.

10.3 Primary Schools

Children under the age of 13 are generally considered not mature enough to fully understand their data rights and the implications of a SAR or general information request. Therefore, in most cases, requests made by parents or carers on behalf of their child may be granted without the child's explicit consent. However, this is not an absolute rule; each child's capacity to understand their rights will be assessed on a case-by-case basis.

10.4 Secondary schools

Children aged 13 and above are generally considered mature enough to understand their data rights and the implications of a SAR or a general information request. Therefore, in most cases, requests made by parents or carers on behalf of a pupil may not be granted without the pupil's explicit consent. However, this is not an absolute rule; each pupil's capacity to understand their rights will be assessed on a case-by-case basis.

10.5 Students 18 and over

Once a student reaches the age of 18, they are considered an adult for GDPR purposes. As such, they can exercise their data protection rights independently, including making SARs and general information requests, without the need for parental consent. The assessment of a student's

capability to manage their data no longer applies, and the student has full control over their personal data and rights under GDPR.

11. Data breaches

In the event of a data breach, the Trust / school follows a structured response plan, including:

- Immediate containment and assessment
- Notification to the DPO
- Reporting to the ICO if required
- Communication with affected individuals, where necessary

11.1 The Trust / School will take all reasonable steps to prevent personal data breaches. In the event of a suspected or actual data breach, the procedures outlined in Appendix 2 will be followed promptly and thoroughly. Any individual who becomes aware of a data breach must report it immediately to a member of the SLT, the Trust-appointed Data Protection Lead, or the CEO.

All breaches will be assessed without delay to determine the level of risk to individuals and whether notification to the ICO and affected individuals is required, in accordance with the UK GDPR and the DPA 2018.

11.2 Where appropriate, the data breach will be reported to the ICO within 72 hours of the Trust becoming aware of it. Examples of reportable breaches include, but are not limited to:

- The publication of a non-anonymised dataset on the Trust/School website, revealing the exam results of pupils eligible for the pupil premium
- Safeguarding information being disclosed to an unauthorised individual
- The theft of a Trust/School laptop containing unencrypted personal data about pupils/students

11.3 A designated member of the Senior Leadership Team (SLT) and the Trust-appointed Data Protection Lead are responsible for maintaining an up-to-date Record of Processing Activities (ROPA) in accordance with Article 30 of the UK GDPR. This record will document all relevant data processing carried out by the Trust/School and will be reviewed regularly to ensure ongoing compliance with data protection legislation.

12. Disposal of information

The Trust ensures that personal data is securely disposed of when it is no longer needed. Personal data that is inaccurate or out of date will also be securely disposed of if it cannot, or does not need to, be rectified or updated. To achieve this, the Trust will:

- Shred or incinerate paper-based records
- Overwrite or permanently delete electronic files
- Use a third party for secure data disposal, where necessary
- When using a third party, the Trust will require sufficient guarantees that the disposal process complies with data protection laws to ensure the secure handling of personal data.

13. Complaints

Complaints will be handled in accordance with the Trust's complaints policy and procedures. If a complaint relates to the handling of personal information, it may be referred to the ICO, the statutory regulator, where appropriate.

14. Training

All staff, trustees, and governors will receive data protection training as part of their induction, ensuring they are aware of their responsibilities as outlined in this policy. Data protection will also be incorporated into ongoing professional development, with all staff required to participate in refresher training at least annually. This training will maintain awareness of their responsibilities and best practices, particularly in response to changes in legislation, guidance, or the Trust's processes.

15. Data Retention

The Trust retains personal data in accordance with the Information and Records Management Society (IRMS) guidance. Personal data is securely destroyed once it is no longer required. See Data Retention Policy.

16. Review and Monitoring

The appointed person within the Trust is responsible for monitoring and reviewing this policy.

The Trust and its schools will maintain a record of all information collected, including details of its destruction and any data breaches, including those that are not reportable.

This policy will be reviewed every two years, or sooner if there are legislative changes, and will be presented to the Board of Trustees for approval. The Trust is committed to continuous monitoring and ensuring compliance with data protection laws.

17. Contact Information

For any queries regarding this policy or data protection matters, please contact the Data Protection Officer. Contact details can be found in Appendix 1.

Appendix 1

Name and contact details of Data Protection Officer:

Name	**TurnItOn**
Address	**Unit 1F, Network Point, Range Road, Witney, Oxon, OX29 0YN**
Email	**office@turniton.co.uk**
Phone	**01865 597620**

Name and contact details of the Trust appointed lead with responsibility for oversight of Data Protection and GDPR:

Name	**Head of Estates and IT**
Address	**c/o Ranelagh School, Ranelagh Drive, Bracknell, Berks, RG12 9AD**
Email	**ithelpdesk@bonitas.org**
Phone	**01344 421233**

Name and contact details of senior leader with responsibility for oversight of Data Protection at Jennett's Park Primary School:

Name	**Elizabeth Savage, Headteacher**
Address	**3 Tawney Owl Square, Jennett's Park, Bracknell Berks, RG12**
Email	**esavage@jennetts.bonitas.org.uk**
Phone	**01344 301269**

Name and contact details of senior leader with responsibility for oversight of Data Protection at Ranelagh School:

Name	**Mark Williams, Deputy Headteacher**
Address	**c/o Ranelagh School, Ranelagh Drive, Bracknell, Berks, RG12 9AD**
Email	**mwilliams@ranelagh.bonitas.org.uk**
Phone	**01344 421233**

Personal Data Breach Procedure

This procedure is based on guidance from the Information Commissioner's Office (ICO) and complies with the UK General Data Protection Regulation (UK GDPR).

1. Reporting a Breach

On discovering or causing a breach (or a potential breach), the staff member or data processor must immediately notify the Data Protection Officer (DPO).

2. Initial Assessment

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

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised persons

3. Internal Notification

The designated senior leader with oversight of data protection, will inform the CEO, Headteacher, Chair of Trustees and Chair of Governors. The DPO will retain independent oversight of the investigation.

4. Containment and Mitigation

The DPO will advise on appropriate steps to contain the breach and minimise its impact. Relevant staff or data processors will take action in line with this advice. Actions specific to certain data types are set out at the end of this procedure

5. Consequence Assessment

The DPO will assess the potential consequences of the breach, considering both their severity and the likelihood of them occurring.

6. Risk Assessment and ICO Notification Decision

The DPO will assess whether the breach must be reported to the ICO, in line with UK GDPR Article 33. This decision will be made on a case-by-case basis and will consider whether the breach is likely to result in a risk or high risk to individuals' rights and freedoms, including possible:

- Loss of control over their data
- Discrimination
- Identity theft or fraud
- Financial loss

- Unauthorised reversal of pseudonymisation (e.g. Key-coding)
- Damage to reputation
- Loss of confidentiality
- Other significant economic or social disadvantage

If there is a likely risk to individuals' rights and freedoms, the DPO must report the breach to the ICO.

7. Documentation of Decision

Whether or not the breach is reported to the ICO, the DPO will record the decision and the rationale behind it. This documentation will be retained as set out in the Information Asset Register (IAR).

8. ICO Notification (if required)

If required, the DPO will notify the ICO via the 'report a breach' page on the ICO website within 72 hours of becoming aware of the breach. The report will include:

- A description of the nature of the breach, including (where possible):
  - the categories and approximate number of individuals affected
  - the categories and approximate number of personal data records affected
- The name and contact details of the DPO
- The likely consequences of the breach
- The measures taken, or proposed, to deal with the breach and mitigate its effects

9. Incomplete Information

If all required information is not yet available within 72 hours, the DPO will submit an initial report with known details, explain the delay, and provide the remaining information as soon as possible.

10. Notification to Data Subjects (if high risk)

If the breach is likely to result in a high risk to individuals' rights and freedoms (Article 34), the DPO will promptly inform affected individuals in writing. This communication will include:

- The name and contact details of the DPO
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to address the breach and mitigate its effects

Notifications may be issued via letter, secure email, or other appropriate means depending on available contact details.

11. Notification to Third Parties

Where necessary, the DPO will inform any relevant third parties who can assist in mitigating the effects of the breach. This may include:

- Police
- Insurers

- Banks or credit card providers
- Local authorities or legal advisers

12. Record-Keeping

The Trust / School will maintain a Data Breach Log, recording all data breaches regardless of whether they are reported to the ICO. For each breach, the log will include:

- Facts and cause of the breach
- Impact and consequences
- Actions taken to contain it
- Measures implemented to prevent recurrence

13. Post-Breach Review

The DPO, Headteacher, and the senior leader with data protection oversight will meet as soon as reasonably possible following the breach to review the incident. This review will consider what went wrong, how it was handled, and how similar breaches can be prevented in the future.

14. Actions for Specific Data Types

Certain data types require tailored responses in the event of a breach:

- **Sensitive or safeguarding data** (e.g. health, SEND, child protection): escalate immediately to the DPO and DSL; notify individuals if appropriate; seek legal/safeguarding advice.
- **Pupil or staff records**: check for third-party data; assess risks to welfare or employment; notify affected individuals.
- **Financial data** (e.g. bank details): inform finance staff; contact banks if needed; report to Action Fraud if fraud is suspected.
- **IT credentials**: reset passwords; audit system access; notify IT support.
- **Misdirected emails**: attempt recall; contact recipient; confirm deletion if data was disclosed.

15. Actions to Minimise Future Risks

The Trust / School will take appropriate actions to reduce the likelihood and impact of future breaches, especially those involving high-risk or sensitive personal data. The effectiveness of these actions will be reviewed and, if necessary, procedures and systems will be further improved.

Related Policy

This procedure should be read in conjunction with the **Trust Data Protection Policy**.

Appendix 3

Procedures for Responding to Subject Access Requests (SARs)

Under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018:

1. Rights of Access to Information

Under UK GDPR, individuals (data subjects) have the right to access personal data that the Trust / School holds about them. This is known as a Subject Access Request (SAR). These rights include:

- Confirmation that their data is being processed
- Access to their personal data
- Supplementary information (such as the purposes of processing, retention periods, and who the data is shared with)

This procedure applies only to SARs under data protection legislation, not requests made under the Education (Pupil Information) Regulations 2005 (England) or other laws.

2. Making a Subject Access Request

Requests must be made in writing (email is acceptable) and addressed to the Headteacher or the Data Protection Officer (DPO). The request should clearly specify what personal data the individual is seeking. If the request is unclear, the school will contact the requester to clarify before proceeding.

3. Identity Verification

Before any data is disclosed, the identity of the requester must be verified. Acceptable proof includes (but is not limited to):

- Passport
- Driving licence
- Recent utility bill (showing name and address)
- Birth or marriage certificate
- Bank or mortgage statement

If the request is made on behalf of a pupil, proof of parental responsibility is also required.

4. Requests on Behalf of a Child

Children aged 13 or over are generally considered to have sufficient capacity to make a SAR themselves, unless proven otherwise. A child with sufficient maturity and understanding has the right to access their own personal data and can refuse consent to a third party, including a parent, accessing their records.

Where the child is not deemed to have capacity to understand their rights, an individual with parental responsibility or legal authority may make the request on their behalf. The data controller must act in the best interests of the child.

Where appropriate, the Headteacher should discuss the request with the child and take their views into account when deciding whether to release their personal data to a third party, including parents or guardians.

5. Timescales

The school must respond to SARs within one calendar month of receipt of the request and proof of identity. This period may be extended by up to two months for complex requests, in which case the requester will be informed of the delay and reason.

6. Reviewing the Information

Before releasing data, the school must review the records and consider:

- Exemptions under the UK GDPR
- Third-party data (data about others)
- Safeguarding or health concerns

7. Third-Party Data

Third-party data is information provided by someone other than the data subject, such as the Police, Local Authority, healthcare professionals, or another school. Before disclosing personal data that identifies another individual, the school must consider whether it is reasonable to disclose it without that person's consent. Where possible, consent should be sought. If consent is not obtained, the school must balance the rights of the data subject with the privacy rights of the third party before deciding whether to redact or disclose.

8. Exemptions from Disclosure

Data may be withheld if disclosure:

- Would cause serious harm to the physical or mental health of the pupil or another person
- Would identify someone at risk of abuse
- Relates to legal proceedings or court reports
- Contains confidential references given or received

If there are concerns about disclosing information, advice should be sought from the DPO before proceeding.

9. Redaction and Record Keeping

Any redactions must be justified and documented. A full unredacted version should be retained securely by the school in case of complaints or audits.

10. Format of Response

The information should be provided in a clear and intelligible format. Any codes, acronyms, or technical terms should be explained. Illegible data should be transcribed or retyped for clarity.

11. Method of Delivery

Information may be provided:

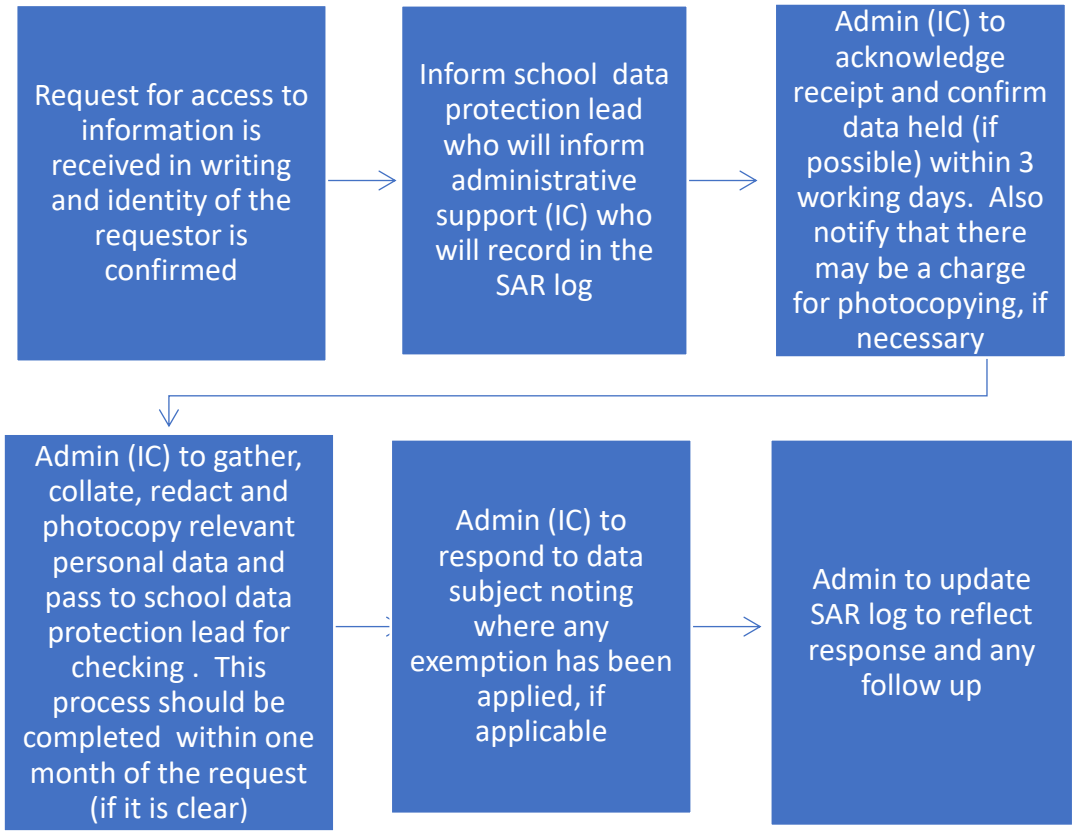
- Electronically
- As hard copy
- At a face-to-face meeting, if requested

If posted, it must be sent by recorded or registered mail. The method of delivery will take into account the applicant's preferences and security considerations.

12. Complaints

If a requester is dissatisfied with the handling of their SAR, they may raise a complaint through the school's complaints policy. They also have the right to complain to the Information Commissioner's Office (ICO): https://www.ico.org.uk

Subject Access Request Procedure



Appendix 4

Subject Access Request Form

I am writing to request access to the personal information you hold about me, in line with my rights under the UK General Data Protection Regulation (UK GDPR).

This request is to help me understand what information you hold about me and to make sure it is being used lawfully.

Under the UK GDPR, the school is required to respond to this request within one calendar month. There should be no charge unless the request is manifestly unfounded or excessive.

School applying to:	
I am making this request for someone else *[Optional]* *Tick this box if you're making this request for someone else eg a child, relative, friend and provide their details.*	☐ Name: Address: Contact Details: Relationship:
Name: [Full name]	
Date:	
Relationship with the school	☐ Pupil ☐ Parent ☐ Employee ☐ Trustees / Governor ☐ Volunteer ☐ Other (please specify)
Correspondence address:	
Contact number:	
Email address:	
Details of the personal information requested: *Please state details of the information required. Please be specific. i.e.* • *My child's personnel file* • *My child's medical records*	

• *Emails between 'A' and 'B'* *Include a time frame {e.g. from xx – to xx dates]* *Details of what you can ask for can be found at: https://ico.org.uk/for-the-public/getting-copies-of-your-information-subject-access-request/*	
Reason for requesting this information [*Optional]* *This may help the school in finding the information you need and can help with a faster response*	
Other details that may help the school find the information *(Optional)* *e.g. Details about what it relates to*.	
I understand that: *[Please tick]*	☐ If the school requires advice on handling this request, it will contact the Information Commissioner's Office on 0303 123 1113 or visit www.ico.org.uk ☐ If the school needs more information from me, it will contact me as soon as possible.
Signed:	
For office use only: *Name:*	Date received:
Proof of ID: *Before any data is disclosed, the identity of the requester must be verified. Acceptable proof includes (but is not limited to):* *If the request is made on behalf of a pupil, proof of parental responsibility is also required.*	☐ Passport ☐ Driving licence ☐ Recent utility bill (showing name and address) ☐ Birth or marriage certificate ☐ Bank statement

Appendix 5

Backup Agreement

1. Recovery from previous version using Shadow Copy for files/ folders accidentally deleted/lost/corrupted is available for approximately four weeks.

2. Real-time replication of the data occurs on two Storage Area Networks. These are in secure air-conditioned server rooms in separate buildings. If one were to fail the data would be available in the other.

3. Hourly backups of data from servers are taken to the Network Attached Storage (NAS) Server. The NAS is a separate server from the data servers and is located in a secure air-conditioned room dedicated to servers with separate power supplies.

4. MIS, SIMS and Finance data is stored on ESS hosted servers.

5. Monthly backups are copied from the backup server to a separate location in another school via a direct fibre link. This data is encrypted using our Quest backup software. There is a Network Attached Storage device in a locked air-conditioned room at this location.

6. System backups of servers are taken when changes are made to the system. Data is recovered periodically from the backup server locations, to ensure the integrity of the backups.

7. Backups of Exchange, OneDrive, SharePoint and Teams Office 365 data are taken on a daily basis using Barracuda Cloud-to-Cloud Backup software and are stored in encrypted cloud storage by the software provider.