GUILSBOROUGH ACADEMY

Data Protection Policy

Policy Name	Data Protection
Committee	Finance Audit and Risk
Owner	Trust Board and Chief Finance Officer
Statutory	Yes
Authorisation	FAR committee to ratify

Date Ratified	Review Date
April 2023	April 2024

Contents

1. Introduction

1.1. Our Multi Academy Trust aims to ensure that all personal data collected about staff, pupils, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

1.2. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

2.1. This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

2.2. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

2.3. This policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
Special categories of personal data	Special category data is personal data which the GDPR says 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	Any action performed on personal data, such as 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 of 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.

4. The data controller

4.1. Our academy processes personal data relating to parents, pupils, staff, trustees, visitors and others, and therefore is a data controller.

4.2. The Multi Academy Trust has paid its data protection fee to the ICO and will pay this annually or as otherwise legally required.

5. Roles and responsibilities

5.1. This policy applies to all staff employed by our academy, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.2 Trust board

The trust board has overall responsibility for ensuring that our academy complies with all relevant data protection obligations.

5.3 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the trust board and, where relevant, report to the board their advice and recommendations on academy data protection issues.

For routine enquiries about this policy, contact the academy's data protection representative in the first instance Mr Niland, Assistant Principal, niland@guilsborough.northants.sch.uk.

The DPO is also a point of contact for individuals whose data the academy processes, and the first point of contact for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is GDPR Sentry Limited and are contactable via support@gdprsentry.com

5.4 Principal

The Principal acts as the representative of the data controller on a day-to-day basis.

5.5 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Multi Academy Trust of any changes to their personal data, such as a change of address
- Contacting the designated school contact, or the DPO, in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure

- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If 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
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

6.1 The GDPR is based on data protection principles that our academy must comply with.

The principles say that personal data must be:

- 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 is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

6.2 This policy sets out how the academy aims to comply with these principles.

7. Collecting personal data

7.1. 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 protection law:
- The data needs to be processed so that the academy can **fulfil a contract** with the individual, or the individual has asked the academy to take specific steps before entering into a contract
- The data needs to be processed so that the academy 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
- The data needs to be processed so that the academy, 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 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**

7.1.1. 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.

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**

- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

7.1.2. For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

7.1.3. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.1.4. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Records Retention Destruction and Archive Policy.

8. Sharing personal data

8.1. We will not normally share personal data with anyone else, but may do so where it is set out in our Privacy Notices or there are certain circumstances where we may be required to do so and:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

8.1.1 We will also share personal data with law enforcement and government bodies where we are legally required to do so.

8.1.2 We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

8.1.3 Where we transfer personal data internationally, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1. Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the academy 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 Mr Niland, Assistant Principal, niland@guilsborough.northants.sch.uk. 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 Mr Niland, Assistant Principal.

9.2. 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 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, subject access requests from parents or carers of pupils aged 12 and below at our academy 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.

9.3. 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.

When a Subject Access Request is made details of the request will be placed in the individuals record and disposed of when the record is disposed of in accordance with the Retention Schedule set out in the Information and Record Management Society's Toolkit for Schools.

9.4. 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)

9.5. Individuals should submit any request to exercise these rights to the contact the Multi Academy Trust's data protection representative in the first instance, Mr Niland, Assistant Principal, niland@guilsborough.northants.sch.uk. If staff receive such a request, they must immediately forward it to contact the Multi Academy Trust's data protection representative or the DPO.

10. Parental requests to see the educational record

10.1. 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.
10.2. If the request is for a copy of the educational record, the Multi Academy Trust may charge a fee to cover the cost of supplying it.
10.3. This right applies as long as the pupil concerned is aged under 18.
10.4. There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. CCTV

11.1. We use CCTV in various locations around the Trust sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.
11.2. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
11.3. Any enquiries about the CCTV system should be directed to Mr Niland, Assistant Principal.

12. Photographs and videos

12.1. 1As part of our academy activities, we may take photographs and record images of individuals within our academy.
12.2. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.
12.3. Uses may include:

- Within academy on notice boards and in academy newsletters, displays, digital signage,
- Outside of academy by external agencies such as the academy photographer, newspapers, campaigns
- Online on our academy website or social media pages

12.4. Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the digital photograph or video and not distribute it further. If consent is withdrawn after a photograph is used in a publication(s) we will continue to make use of the publication(s) incorporating the photograph but we will not use the photograph again and will remove it from the publication if it is re-printed
12.5. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.
12.6. See our safeguarding policy for more information on our use of photographs and videos.
12.7. Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

13. Data protection by design and default

13.1. We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our Multi Academy Trust contact and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data will not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

- Passwords that are a complex t or three-words and the use of Multi-Factor authentication are used to access academy computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or trustees who store personal information on their personal devices are expected to follow the same security procedures as for academy-owned equipment (see our acceptable use policy).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

15.1. Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

15.2. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15.3. All data will be kept in accordance with the Retention Schedule set out in the Information and Record Management Society's Toolkit for Schools.

16. Personal data breaches

16.1. The academy will make all reasonable endeavours to ensure that there are no personal data breaches.

16.2. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

16.3. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in the academy context may include, but are not limited to:

- A non-anonymised dataset being published on the academy website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of an academy laptop containing non-encrypted personal data about pupils

17. Training

17.1. All staff and trustees are provided with data protection training as part of their induction process.

17.2. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the academy's processes make it necessary.

18. Monitoring arrangements

18.1. The Assistant Principal and DPO are responsible for monitoring and reviewing this policy.

18.2. This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our academy's practice. Otherwise, or from then on, this policy will be reviewed every year and shared with the full trust board.

19. Links with other policies

19.1. This data protection policy is linked to our:

- Records Retention Destruction and Archive Policy

- Privacy Notices
- Freedom of information publication scheme
- Safeguarding Policy
- ICT Acceptable Use Policy
- CCTV Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify Mr Niland, Assistant Principal, or the DPO
- The Multi Academy Trust's data protection representative and DPO will investigate the report, and determine whether a breach has occurred. To decide, they 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 people
- The Multi Academy Trust's data protection representative and DPO will alert the Principal and the chair of trustees
- The Multi Academy Trust's data protection representative and the DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The Multi Academy Trust's data protection representative and the DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the academy's computer network.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the academy's computer network.

- The DPO and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the appropriate action to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.