DATA PROTECTION POLICY

ORIGINATOR: Oliver Teasel
SLT LINK: Stuart Williams

RUTLAND AND DISTRICT SCHOOLS' FEDERATION

February 2024

CONTENTS

1. INTRODUCTION 2
2. LEGISLATION AND GUIDANCE 2
3. DEFINITIONS 2
4. THE DATA CONTROLLER 3
5. ROLES AND RESPONSIBILITIES 3
6. DATA PROTECTION PRINCIPLES 4
7. PROCESSING PERSONAL DATA 5
8. SHARING PERSONAL DATA 6
9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS 7
10. CCTV 9
11. PHOTOGRAPHS AND VIDEOS 9
12. DATA SECURITY AND STORAGE OF RECORDS 10
13. DISPOSAL OF RECORDS 10
14. PERSONAL DATA BREACHES 10
15. TRAINING 10

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE 11

1. INTRODUCTION

The Rutland and District Schools' Federation ('the Federation') collects and uses certain types of personal information about staff, students, parents and other individuals who come into contact with the Federation in order to provide education and associated functions.

Our aim is to ensure that all personal data is collected, stored and processed in accordance with UK data protection law.

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

2. LEGISLATION AND GUIDANCE

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

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

In addition, this policy complies with our funding agreement and articles of association.

3. DEFINITIONS

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
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

	• Health – physical or mental • Sex life or sexual orientation. The Federation does not intend to seek or hold sensitive personal data about staff and students except where the Federation has been notified of the information. Staff or students are under no obligation to disclose to the Federation their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and/or parenthood are needed for other purposes e.g. pension entitlements).
Processing	Anything done to 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

The Trust processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

5. ROLES AND RESPONSIBILITIES

This policy applies to all staff employed by the Trust, and to external organisations or individuals working on our behalf.

5.1 The Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the schools within the Trust comply with all relevant data protection obligations.

5.2 Data Protection Officer

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

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

Our DPO is Oliver Teasel and is contactable via email: oteasel@haringtonschool.com

5.3 All staff

Staff 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
- Contacting 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 UK
  - 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

The UK GDPR is based on data protection principles that our Trust 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.

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

7. PROCESSING 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 Trust can fulfil a contract with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. 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 or exercise its official authority
- The data needs to be processed for the legitimate interests of the Trust (where the processing is not for any tasks the Trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/guardian when appropriate in the case of a student) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/guardian when appropriate in the case of a student) 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.

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/guardian when appropriate in the case of a student) 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.

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.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anoymised. This will be done in accordance with the Trust's record retention schedule.

8. SHARING PERSONAL DATA

8.1 We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a student or parent/guardian 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 students – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK 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.

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

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 students or staff.

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

8.2 Safeguarding

This policy does not prevent or limit the sharing of information for the purpose of keeping children safe. The Federation will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the Designated Safeguarding Lead (DSL) will ensure that they record the following information:

- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent/guardian.

8.3 Privacy Notices

The Federation will issue Privacy Notices as required, informing Data Subjects (or their parents depending on the age of the student) about the personal information that is collected, how the data is used, for what purpose and the length of retention.

9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 Subject access requests

Anybody who makes a request to see any personal information held about them by the Federation is making a subject access request.

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

All subject access requests should be sent to the Data Protection Officer and must be dealt with in full, without delay and at the latest within one month of receipt. If there are likely to be any delays to responding to subject access requests (e.g. requests received during the summer holidays) this should be explained.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or guardians. For a parent or guardian to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or guardians of students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Federation must have written evidence that the individual has authorised the person to make the application.

9.3 Responding to subject access requests

When responding to requests, we may ask for clarity regarding the specific nature of the request (e.g., time-frames or whether to include data that has already been sent previously such as academic reports)

There may be some occasion where we cannot disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the Federation intends to apply any of these exemptions, we will usually explain which exemption and why.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will consider whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts. All files will be reviewed by the Data Protection Officer before any information is sent.

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, individuals also have the right to:

- Withdraw their consent to processing at any time (and where there is no legal basis for the processing)
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)

- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO.

10. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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.

Any enquiries about the CCTV system should be directed to Simon Mellors, Operations Director.

11. PHOTOGRAPHS AND VIDEOS

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/guardians, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/guardian and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

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.

See our Federation Privacy Notice for Students policy for more information on our use of photographs and videos.

12. 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:

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Access to the school network requires password that are regularly updated and two factor authentication where possible.
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT Code of Conduct 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
- Ensuring that colleagues only have access to the personal information they are authorised to access as part of their job
- Not store personal information on local drives or on personal devices.

13. DISPOSAL OF RECORDS

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.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.

14. PERSONAL DATA BREACHES

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.

15. TRAINING

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

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

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by speaking to him direct. If he is unavailable an email explaining the nature of the breach should be sent to oteasel@haringtonschool.com
- The DPO will investigate the report, and determine whether a 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 people
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions).
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Executive Principal.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored as a secure Google Doc ("Personal Data Security Breach Log") Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. 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 of the school's awareness of the breach. 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
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
  - A description, in clear and plain language, of the nature of the personal data breach
  - 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 consider, in light of the investigation and any engagement with affected individuals, whether to 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)
- The DPO and Executive 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.