Royal School for the Deaf Derby

Data Protection Policy

Date of last review:	Spring 2024	**Date of next review:**	Autumn 2025

Policy review dates and changes

Review date	By whom	Summary of changes made	Date implemented
Spring 2024	PB	Protection of Biometric Information	Spring 2024

Signed		**Designation**	Chair of Governors
Name	Janet Hall Heather Flockton	**Date**	Spring 2024

1. Introduction

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 and the 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.

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

2. Definitions used by RSDD

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
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Processing -Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data controller - The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The school is registered with the Information Commissioner's Office (ICO), as legally required.

Data subject - Any living individual who is the subject of personal data held by an organisation.

3. Links to GDPR

The UK General Data Protection Regulation (UK GDPR) works with the Data Protection Act 2018 (DPA 2018) to form the UK's data protection framework. It determines how people's personal data is processed and kept safe, and the legal rights individuals have over their own data. 'Personal data' means information that can identify a living individual.

Changes after Brexit

The UK adopted the EU's GDPR in 2018, but since the UK's withdrawal from the EU it has used its own version, known as the UK GDPR.

Key principles

The GDPR sets out the key principles that all personal data must be processed in line with.

- Data must be: processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected
- There are also stronger rights for individuals regarding their own data.
- The individual's rights include: to be informed about how their data is used, to have access to their data, to rectify incorrect information, to have their data erased, to restrict how their data is used, to move their data from one organisation to another, and to object to their data being used at all

Main requirements

The main requirements are:

- Schools must appoint a data protection officer, who will advise on compliance with the GDPR and other relevant data protection law
- Privacy notices must be in clear and plain language and include some extra information – the school's 'legal basis' for processing, the individual's rights in relation to their own data
- Schools have a month to comply with subject access requests, and in most cases can't charge
- Where the school needs an individual's consent to process data, this consent must be freely given, specific, informed and unambiguous
- There are special protections for children's data
- The Information Commissioner's Office must be notified within 72 hours of a data breach if the breach puts people at risk
- Organisations have to demonstrate how they comply with the new law
- Schools need to carry out a data protection impact assessment when considering using data in new ways, or implementing new technology to monitor pupils
- Higher fines for data breaches

4. Roles and responsibilities

Governors

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

Data Protection Officer (DPO)

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

Our DPO is the Headteacher headteacher@rsdd.org.uk

Headteacher

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

All staff - Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school 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 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

5. Data protection principles

The GDPR is based on data protection principles that our school 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 school aims to comply with these principles.

6. Collecting personal data

Lawfulness, fairness and transparency

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

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

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

- 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

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

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

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.

Limitation, minimisation and accuracy

RSDD 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 anonymised. This will be done in accordance with the school's record retention schedule.

7. Sharing personal data

RSDD 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 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

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

8. Subject access requests and other rights of individuals

Subject access requests

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include

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

If staff receive a subject access request in any form they must immediately forward it to the DPO.

Children and subject access requests

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

Responding to subject access requests

When responding to requests, we

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)

- 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 onerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- 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 request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account 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.

Other data protection rights of the individual

In addition to the right to make a subject access request 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
- 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. If staff receive such a request, they must immediately forward it to the DPO.

9. Parental requests to see the educational record

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

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it. This right applies as long as the pupil concerned is aged under 18.
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.

10. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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 the Headteacher.

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/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.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils 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/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

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 (or pupils where appropriate) have agreed to this.
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, including BSL Newsround

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.

12. The Protection of Biometric Information on Children in Schools

Biometric data is a type of Special Category Date in that its purpose is to uniquely identify a person. Examples include facial imagery, voice recognition and fingerprint technology.. If used, it must be kept safe and must meet the requirements set out in Articles 6 and 9 of the UK GDPR. Consent from parents or carers of children under 18 must be obtained. In addition, the pupil themselves can refuse. **RSDD does not collect or use biometric information.**

13. Data protection by design and default

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 external expert 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
- Completing data protection 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 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 school 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, 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 must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils 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 acceptable use agreement/policy on acceptable use)
- 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

15. 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. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The school 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. Such breaches in a school context may include, but are not limited to

- A non-anonymised dataset being published on the school 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 a school laptop containing non-encrypted personal data about pupils
-

17. 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.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed every two years and shared with the full governing board.

19. See also

- CCTV Policy
- Safeguarding Policy
- E Safety Policy
- Self-declaration criminal record checks

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)
- 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). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Headteacher and the Chair of Governors
- 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 (e.g. from IT providers).
- 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 it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system. See form Appendix 2
- 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)

Records of all breaches will be on the school's computer system
The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
The DPO and Headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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.

Sensitive information being disclosed via email (including safeguarding records)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the external IT support provider to attempt to recall it from external recipients and remove it from the school's email system
In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners

Royal School for the Deaf Derby

Appendix 2 Personal data breach form

Date	
Name	
Role	
Description of Breach	
Categories of individuals affected	
Cause of the breach	
Effects	
Reported to ICO?	
Why / Why not?	Self-assessment as below 1. Have you determined whether a PDB has occurred? 2. Making your own assessment, does the breach involve the personal data of living individuals? 3. Following your own assessment, is there likely to be a high risk to individuals' rights and freedoms? 4. How likely is it that the breach will result in a risk to individuals? Overall risk and need to report to ICO
Were individuals informed?	
Action taken to control the breach	
Actions to stop the breach happening again	
Additional notes	
Person filling in form and role and date completed	

Appendix 3 Security of local and wide area networks

Scope

- All users of the RSDD's wireless notebook computers and other mobile devices are within the scope of this procedure.

Responsibilities

- LEAD IT with Headteacher is responsible for specifying and/or providing the firewalls, anti-malware software, automatic updating, connectivity and backup facilities required under this procedure.
- All users have specific responsibilities in terms of their User Agreements.

Procedure

- RSDD requires notebook computer level deployment of the company's specified firewalls, anti-malware software, and automatic updating facilities that are all up to date [and meet the corporate minimum standards, which are specified and in the User Agreement. (see E Safety Policy)
- RSDD requires notebook computer level deployment of the corporate policy on usernames and passwords, to have a password protected screensaver, and to Password protect/encrypt all folders containing confidential corporate information, and to disable folder and printer sharing, all of which is specified in the User Agreement.
- RSDD requires notebook computers that carry personal data, or are able to connect to systems that store or process personal data, use full-disk encryption. RSDD's full-disk encryption solution is Bitlocker.
- RSDD requires that notebook computers are physically protected against theft and damage while in transit, in storage or in use and that, in cases of loss or theft, the specified corporate policy (see User Agreement) for dealing with such incidents is followed.
- RSDD requires users (in the User Agreement) to ensure that all the most recent operating system and application security-related patches, fixes and updates have been installed.
- RSDD requires (in the User Agreement) that notebook computers are backed up in line with corporate specification.
- RSDD requires users of notebook computers to carry with them at all times the chargers specified in the User Agreement.
- RSDD requires users to comply with the corporate requirements on the means of connecting to public access points, and accessing corporate information, both as described in the User Agreement.
- RSDD requires users, as in the User Agreement, to act with care in public places so as to avoid the risk of screens and confidential notebook computer activity being overlooked by unauthorised persons.
- RSDD carries out regular and ad hoc audits of all notebook computers to ensure that they are configured in compliance with this procedure.
- RSDD provides users with appropriate training and awareness to ensure that they understand the risks of wireless on the road computing and that they understand and can carry out their agreed security obligations.

Appendix 4 Secure Disposal of Storage Media Procedure

Scope

- RSDD requires that all removable storage media are clean (which means it is not possible to read or reconstitute the information that was stored on the device or document) prior to disposal.

Responsibilities

- The Information Security Manager is responsible for managing the secure disposal of all storage media in line with this procedure when they are no longer required.
- All owners of removable storage media are responsible for ensuring that these media are disposed of in line with this procedure.

Procedure

- Hard disks must be cleared of all software and all organisational confidential and restricted information prior to disposal or reuse
    - In the event that hard disks/media contain personal data, and it cannot be removed, then:
        - Review whether or not you really do need to keep an archive within which this personal data is stored; it may well be that there is no overriding business reason for the archive in the first place.
        - If you currently cannot technically delete archived data that is beyond its retention date, then to the hard disk/media needs to be put securely beyond use.
- The Information Security Manager is responsible for the secure disposal of storage media and the disposal of all information processing equipment is routed through their office. A log is retained showing what media were destroyed and/or disposed of, and when. The information asset inventory and/or data inventory is adjusted once the asset has been disposed of.
- Hard disks are cleaned and a WEEE and hardware destruction certification is issued.
- Devices containing confidential information dependent on a risk assessment are destroyed prior to disposal and are never reused.
- Devices containing confidential information that are damaged are subject to a risk assessment prior to sending for repair, to establish whether they should be repaired or replaced.
- Portable or removable storage media of any description are destroyed prior to disposal.
- All media are disposed of in line with regulations on disposal of computer equipment, through RSDD's approved contractor.
- Documents containing confidential] and restricted information that are to be destroyed are shredded by their owners, using a shredder with an appropriate security classification. These shredders are located around the site. The waste is removed by the approved contractor.

Royal School for the Deaf Derby

Appendix 5 Privacy Notice Procedure Staff, Pupils and job applicants

Employee Privacy Notice

NOTE: The wording in this document reflects the requirements of the General Data Protection Regulation (GDPR)

Data controller: RSDD Governing Body. Contact: Clerk to the Governors nicola.hardy@rsdd.org.uk
Data protection officer: Headteacher- Helen Shepherd – headteacher@rsdd.org.uk

The School collects and processes personal data relating its employees to manage the employment relationship. The School is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the School collect?

The School collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender
- the terms and conditions of your employment
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the School
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover
- details of your bank account and national insurance number
- information about your marital status, next of kin, dependants and emergency contacts
- information about your nationality and entitlement to work in the UK
- information about your criminal record
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
- assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence
- information about medical or health conditions, including whether or not you have a disability for which the School needs to make reasonable adjustments; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable)

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

The School may collect this information in a variety of ways. For example, data might be collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the School may collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law.
Data will be stored in a range of different places, including in your personnel file, in the School's HR management systems and in other IT systems (including the School's email system).

Why does the School process personal data?

The School needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.
In some cases, the School needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.
In other cases, the School has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the School to

- run recruitment and promotion processes
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the School complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration
- provide references on request for current or former employees
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities).
Where the School processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring.

Who has access to data?

Your information may be shared internally, including with members of the HR and recruitment team (including payroll), your line manager, managers in the department in which you work and IT staff if access to the data is necessary for performance of their roles.

The School shares your data with third parties in order to [obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. The School may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.
The School also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits and the provision of occupational health services.
The School will not transfer your data to countries outside the European Economic Area.

How does the School protect data?
The School takes the security of your data seriously. The School has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.
Where the School engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long does the School keep data?

The School will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are determined by relevant retention periods for the purposes of responding to enquiries from Statutory Bodies such as HMRC

Your rights

As a data subject, you have a number of rights. You can

- access and obtain a copy of your data on request
- require the School to change incorrect or incomplete data
- require the School to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing
- object to the processing of your data where the School is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact headteacher@rsdd.org.uk
If you believe that the School has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You have some obligations under your employment contract to provide the School with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the School with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.
Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the School to enter a contract of employment with you. If you do not provide other information, this will hinder the School's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based on automated decision-making.

The Law Relating to this document

Leading statutory authority
General Data Protection Regulation (2016/679 EU)
Data Protection Bill

The General Data Protection Regulation (GDPR) requires employers to be transparent about the personal data that they hold and how it is used. The GDPR requires employers to provide the following information to employees at the point that data is collected from them:

- the identity and contact details of the School
- the purposes for which the personal data will be processed, as well as the legal basis for the processing
- if the employer is relying on its legitimate interests as the lawful condition for processing, what those legitimate interests are
- the recipients or categories of recipients of the personal data
- any transfer of the data outside the European Economic Area and the basis for such transfer
- the period for which data will be stored, or the criteria used to determine how long data will be retained
- the individual's rights to subject access, rectification or erasure of personal data, and the right to restrict processing or object to processing
- the right to withdraw consent to processing at any time, if the data controller is relying on consent as a ground for processing
- the right to lodge a complaint with the Information Commissioner
- whether or not providing the data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and whether or not the data subject is obliged to provide the personal data, and the consequences of failing to provide the data
- the existence of any automated decision-making and meaningful information about the logic involved and the consequences of any such processing for the individual; and
- where data is obtained from a third party, the source of the data, including if it came from publicly accessible sources.

Employers are required to provide the information in a concise, transparent, intelligible and easily accessible form. It must be in writing, and written in clear and plain language.
Where an employer wishes to process existing personal data for a new purpose, it must inform the employee of that further processing.
Schools are required to appoint a data protection officer under the GDPR if they are a public authority, if their core activities include the regular and systemic monitoring of data subjects on a large scale, or if their core activities consist of processing special categories of personal data or data relating to criminal convictions and offences on a large scale.
The GDPR and the Data Protection Bill place restrictions on the processing of special categories of personal data and data on criminal convictions and offences. Under the GDPR, special categories of personal data are defined as information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data. Data on criminal convictions and offences includes information relating to criminal allegations and proceedings. These types of data were previously known as "sensitive personal data" under the Data Protection Act 1998.
In order to process special categories of employment data, such as disability information, or data on criminal convictions and offences employers are likely to rely on the ground that processing is necessary to perform or exercise obligations or rights under employment law.
Where an employer collects employee data for equal opportunities monitoring purposes, it may rely on a limited exception under the Data Protection Bill for processing data related to racial or ethnic origin, sexual orientation, health and religious or belief only. Alternatively, in limited circumstances, the employer may choose to ask for employee consent where processing is entirely optional (eg for employee support networks or employee wellness programs).

Complaints

We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.
To make a complaint, please contact our data protection officer.
Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Privacy notice for pupils

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data. This privacy notice explains how we collect, store and use personal data about you. We, RSDD, are the 'data controller' for the purposes of data protection law.

The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at school.
For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.
This information includes:

- Your contact details
- Your test results
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Photographs
- CCTV images

Why we use this data

We use this data to help run the school, including to:

- Get in touch with you and your parents when we need to
- Check how you're doing in exams and work out whether you or your teachers need any extra help
- Track how well the school as a whole is performing
- Look after your wellbeing

Our legal basis for using this data

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.
Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information

While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.
We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store this data

We will keep personal information about you while you are a pupil at our school. We may also keep it after you have left the school, where we are required to by law.
We have a records retention policy which sets out how long we must keep information about pupils.

Data sharing

We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.
Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- Our local authority – to meet our legal duties to share certain information with it, such as concerns about pupils' safety and exclusions
- The Department for Education (a government department)
- Your family and representatives
- Educators and examining bodies
- Our regulator (the organisation or "watchdog" that supervises us), ([specify as appropriate, e.g. Ofsted, Independent Schools Inspectorate]
- Suppliers and service providers – so that they can provide the services we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database

We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.
Some of this information is then stored in the National Pupil Database, which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.
The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.
The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.
You can find more information about this on the Department for Education's webpage on how it collects and shares research data.
You can also contact the Department for Education if you have any questions about the database.

Youth support services

Once you reach the age of 13, we are legally required to pass on certain information about you to the local authority and/or youth service provider as it has legal responsibilities regarding the education or training of 13-19 year-olds.
This information enables it to provide youth support services, post-16 education and training services, and careers advisers.
Your parents/carers, or you once you're 16, can contact our data protection officer to ask us to only pass your name, address and date of birth to the local authority and/or youth service provider.

Transferring data internationally

Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

Your rights

How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a **'subject access request'**, as long as we judge that you can properly understand your rights and what they mean.
If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.
If you want to make a request, please contact our data protection officer.

Your other rights over your data

You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.
You can make a complaint at any time by contacting our data protection officer.
You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact the school office.

Privacy notice for parents/carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**.

We, RSDD are the 'data controller' for the purposes of data protection law.

Our data protection officer is Helen Shepherd headteacher@rsdd.org.uk

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing
- Provide a services to parents and carers to monitor student progress
- Communicate with parents and carers via various communication platforms

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Our records retention policy sets out how long we keep information about pupils.

To view our policy please request a copy of policy GDPR Doc 2.4 from the school office.

Data sharing

We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education
- The pupil's family and representatives
- Educators and examining bodies
- Our regulator [specify as appropriate, e.g. Ofsted, Independent Schools Inspectorate]
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census and early years' census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.

You can also contact the Department for Education with any further questions about the NPD.

Youth support services

Once our pupils reach the age of 13, we are legally required to pass on certain information about them to the local authority and/or youth service provider as they have legal responsibilities regarding the education or training of 13-19 year-olds.
This information enables it to provide youth support services, post-16 education and training services, and careers advisers.
Parents/carers, or pupils once aged 16 or over, can contact our data protection officer to request that we only pass the individual's name, address and date of birth to the local authority and/or youth service provider.

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.
Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.
Parents also have the right to make a subject access request with respect to any personal data the school holds about them.
If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.
If you would like to make a request please contact our school office.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.
To make a complaint, please contact our data protection officer.
Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113

- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our school office.

Job Applicant Privacy Notice

Data controller: RSDD Governing Body. Contact: Clerk to the Governors nicola.hardy@rsdd.org.uk

Data protection officer: Headteacher- Helen Shepherd – headteacher@rsdd.org.uk

As part of any recruitment process, the School collects and processes personal data relating to job applicants. The School is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the School collect?

The School collects a range of information about you. This includes

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the School needs to make reasonable adjustments during the recruitment process;
- Information about previous convictions (spent or not) and disqualifications
- information about your entitlement to work in the UK; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

The School may collect this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment

The School may also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks. Where the School seeks information from third parties it will inform you that it is doing so.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why does the School process personal data?

The School needs to process data to take steps at your request prior to entering into a contract with you. It may also need to process your data to enter into a contract with you.

In some cases, the School needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

The School has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the School to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The School may also need to process data from job applicants to respond to and defend against legal claims.

The School may process information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to employment.

The School processes other special categories of data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is for equal opportunities monitoring purposes.

For some roles, the School is obliged to seek information about criminal convictions and offences including disqualifications under the Childcare (Disqualification) Regulations 2009, Teacher Prohibition and Section 128 Directions. Where the School seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

The School will not use your data for any purpose other than the recruitment exercise for which you have applied.

Who has access to data?

Your information may be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, senior leaders of the School and members of the Governing Body and IT staff if access to the data is necessary for the performance of their roles.

The School will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. The School will then share your data with employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

The School will not transfer your data outside the European Economic Area unless an overseas check is required to satisfy safeguarding checks in recruitment, selection and assessment. Should this be necessary the School will seek your consent which may be withdrawn at any time.

How does the School protect data?

The School takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties

For how long does the School keep data?

If your application for employment is unsuccessful, the School will hold your data on file for no longer than one month after the end of the relevant recruitment process. If you agree to allow the School to keep your personal data on file, the Schools will hold your data on file for a further 3 month period for consideration for future employment opportunities. At the end of that period or on notice of withdrawal (whichever is the sooner) your data is deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the School to change incorrect or incomplete data;
- require the School to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the School is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact the data protection officer:
Headteacher- Helen Shepherd – headteacher@rsdd.org.uk

If you believe that the School has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to the School during the recruitment process. However, if you do not provide the information, the School may not be able to process your application properly or at all.

Automated decision-making

Recruitment processes are not based on automated decision-making.

Relevant legislation

General Data Protection Regulation (2016/679 EU)
Data Protection Bill

The General Data Protection Regulation (GDPR) requires employers to be transparent about the personal data that they hold and how it is used. The GDPR requires employers to provide the following information to job applicants at the point that data is collected from them:

- the identity and contact details of the School;
- the contact details of the data protection officer, if relevant;
- the purposes for which the personal data will be processed, as well as the legal basis for the processing;
- if the employer is relying on its legitimate interests as the lawful condition for processing, what those legitimate interests are;
- the recipients or categories of recipients of the personal data;

- any transfer of the data outside the European Economic Area and the basis for such transfer;
- the period for which data will be stored, or the criteria used to determine how long data will be retained;
- the individual's rights to subject access, rectification or erasure of personal data, and the right to restrict processing or object to processing;
- the right to withdraw consent to processing at any time, if the data controller is relying on consent as a ground for processing;
- the right to lodge a complaint with the Information Commissioner;
- whether or not providing the data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and whether or not the data subject is obliged to provide the personal data, and the consequences of failing to provide the data;
- the existence of any automated decision-making and meaningful information about the logic involved and the consequences of any such processing for the individual; and
- where data is obtained from a third party, the source of the data, including if it came from publicly accessible sources.

Employers are required to provide the information in a concise, transparent, intelligible and easily accessible form. It must be in writing, and written in clear and plain language.
Where an employer wishes to process existing personal data for a new purpose, it must inform the job applicant of that further processing.

Schools are required to appoint a data protection officer under the GDPR if they are a public authority, if their core activities include the regular and systemic monitoring of data subjects on a large scale, or if their core activities consist of processing special categories of personal data or data relating to criminal convictions and offences on a large scale.

The GDPR and the Data Protection Bill place restrictions on the processing of special categories of personal data and data on criminal convictions and offences. Under the GDPR, special categories of personal data are defined as information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data. Data on criminal convictions and offences includes information relating to criminal allegations and proceedings. These types of data were previously known as "sensitive personal data" under the Data Protection Act 1998.

In order to process special categories of employment data, such as disability information, or data on criminal convictions and offences of job applicants, employers are likely to rely on the ground that processing is necessary to perform or exercise obligations or rights under employment law. Where an employer collects applicant data for equal opportunities monitoring purposes, it may rely on a limited exception under the Data Protection Bill for processing data related to racial or ethnic origin, sexual orientation, health and religious or belief only.

This document refers to data being collected from third-party sources such as former employers, background check providers or the Disclosure and Barring Service. If data is obtained from other third-party sources, the data controller will have to provide additional information, including the categories of data being processed and the source of the data.