Royal School for the Deaf Derby

General Data Protection Regulation (GDPR) Policy

Date of last review:	Nov 2020	**Date of next review:**	Sep 2023

Policy review dates and changes

Review date	By whom	Summary of changes made	Date implemented

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

1. Introduction

1.1 Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.2 Definitions used by the organisation (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

1.3 Article 4 definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

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.

Data subject – any living individual who is the subject of personal data held by an organisation.

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.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or

otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.
Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.
Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.
Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2. Policy statement

2.1 The Board of Governors and management of Royal School for the Deaf Derby, located at Royal School for the Deaf Derby, 180 Ashbourne Rd, Derby DE22 3BH are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the “rights and freedoms” of individuals whose information Royal School for the Deaf Derby collects and processes in accordance with the General Data Protection Regulation (GDPR).

2.2 Compliance with the GDPR is described by this policy and other relevant policies along with connected processes and procedures.

2.3 The GDPR and this policy apply to all of Royal School for the Deaf Derby’s personal data processing functions, including those performed on customers’, clients’, employees’, suppliers’ and partners’ personal data, and any other personal data the organisation processes from any source.

2.4 Royal School for the Deaf Derby has established objectives for data protection and privacy, which are in PIMS and GDPR Objectives Record (GDPR REC 4.11).

2.5 Data Protection Officer is responsible for reviewing the register of processing annually in the light of any changes to Royal School for the Deaf Derby’s activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority’s request.

2.6 This policy applies to all Employees/Staff of Royal School for the Deaf Derby such as outsourced suppliers. Any breach of the GDPR or this PIMS will be dealt with under Royal School for the Deaf Derby’s disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.7 Partners and any third parties working with or for Royal School for the Deaf Derby, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Royal School for the Deaf Derby without having first entered into a data confidentiality agreement which can be found on the Royal School for the Deaf Derby portal. Which imposes on the third party obligations no less onerous than those to which Royal School for the Deaf Derby is committed, and which gives Royal School for the Deaf Derby the right to audit compliance with the agreement.

To support compliance with the GDPR, the Board of Governors has approved and supported the development, implementation, maintenance and continual improvement of a documented personal information management system ('PIMS') for Royal School for the Deaf Derby.
All Employees/Staff of Royal School for the Deaf Derby and any other external parties identified by PIMS are expected to comply with this policy and with the PIMS that implements this policy. All Employees/Staff, and certain external parties, will receive appropriate training. The consequences of breaching this policy are set out in Royal School for the Deaf Derby's disciplinary policy and in contracts and agreements with third parties.
In determining its scope for compliance with BS 10012:2017 and the GDPR, Royal School for the Deaf Derby considers:

- any external and internal issues that are relevant to the purpose of Royal School for the Deaf Derby and that affect its ability to achieve the intended outcomes of its PIMS;
- specific needs and expectations of interested parties that are relevant to the implementation of the PIMS;
- organisational objectives and obligations;
- the organisations acceptable level of risk; and
- any applicable statutory, regulatory or contractual obligations.

Royal School for the Deaf Derby's objectives for compliance with the GDPR and a PIMS:

- are consistent with this policy
- are measurable
- take into account GDPR and BS 10012:2017 privacy requirements and the results from risk assessments and risk treatments
- are monitored, communicated and updated as appropriate

Royal School for the Deaf Derby documents those objectives in the PIMS and GDPR Objectives Record (GDPR REC 4.11).

In order to achieve these objectives, Royal School for the Deaf Derby has determined:

- what will be done
- what resources will be required
- who will be responsible
- when it will be completed
- how the results will be evaluated

3. Responsibilities and roles under the General Data Protection Regulation

3.1 Royal School for the Deaf Derby is a data controller and data processor under the GDPR.

3.2 Top Management and all those in managerial or supervisory roles throughout Royal School for the Deaf Derby are responsible for developing and encouraging good information handling practices within Royal School for the Deaf Derby; responsibilities are set out in individual job descriptions.

3.3 Data Protection Officer (DPO) is accountable to Board of Governors of Royal School for the Deaf Derby for the management of personal data within Royal School for the Deaf Derby and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.3.1 development and implementation of the GDPR as required by this policy; and

3.3.2 security and risk management in relation to compliance with the policy.

3.4 Data Protection Officer, who the Board of Governors considers to be suitably qualified and experienced, has been appointed to take responsibility for Royal School for the Deaf Derby's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that Royal School for the Deaf Derby complies with the GDPR, as do Manager/Executive (generic/line)'s in respect of data processing that takes place within their area of responsibility.

3.5 The Data Protection Officer have specific responsibilities in respect of procedures such as the Subject Access Request Procedure (GDPR DOC 2.2) and are the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

3.6 Compliance with data protection legislation is the responsibility of all Employees/Staff of Royal School for the Deaf Derby who process personal data.

3.7 Royal School for the Deaf Derby's Continual Professional Development Policy sets out specific training and awareness requirements in relation to specific roles and Employees/Staff of Royal School for the Deaf Derby generally.

3.8 Employees/Staff of Royal School for the Deaf Derby are responsible for ensuring that any personal data about them and supplied by them to Royal School for the Deaf Derby is accurate and up-to-date.

4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Royal School for the Deaf Derby's policies and procedures are designed to ensure compliance with the principles.

4.1 Personal data must be processed lawfully, fairly and transparently
Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.
Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.
The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.
Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.
Royal School for the Deaf Derby's Privacy Notice Procedure is set out in Appendix 10
The specific information that must be provided to the data subject must, as a minimum, include:
4.1.1 the identity and the contact details of the controller and, if any, of the controller's representative;
4.1.2 the contact details of the Data Protection Officer;
4.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4.1.4 the period for which the personal data will be stored;
4.1.5 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
4.1.6 the categories of personal data concerned;
4.1.7 the recipients or categories of recipients of the personal data, where applicable;
4.1.8 where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
4.1.9 any further information necessary to guarantee fair processing.

4.2 Personal data can only be collected for specific, explicit and legitimate purposes
Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of Royal School for the Deaf Derby's GDPR register of processing.

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing

4.3.1 The Data Protection Officer is responsible for ensuring that Royal School for the Deaf Derby does not collect information that is not strictly necessary for the purpose for which it is obtained
4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the Data Protection Officer
4.3.3 The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by Internal Audit to ensure that collected data continues to be adequate, relevant and not excessive
4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay
4.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
4.4.2 The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
4.4.3 It is also the responsibility of the data subject to ensure that data held by Royal School for the Deaf Derby is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.
4.4.4 Staff / Pupil's parents / carers / Suppliers should be required to notify Royal School for the Deaf Derby of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are located on the Royal School for the Deaf Derby portal. It is the responsibility of Royal School for the Deaf Derby to ensure that any notification regarding change of circumstances is recorded and acted upon.
4.4.5 The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
4.4.6 On at least an annual basis, the Data Protection Officer will review the retention dates of all the personal data processed by Royal School for the Deaf Derby, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure (GDPR-C DOC 11.2.7).
4.4.7 The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month (Subject Access Request Procedure GDPR DOC 2.2). This can be extended to a further two months for complex requests. If Royal School for the Deaf Derby decides not to comply with the request, the Data Protection Officer / GDPR Owner must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.
4.4.8 The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.
4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
4.5.1 Where personal data is retained beyond the processing date, it will be encrypted in order to protect the identity of the data subject in the event of a data breach.
4.10.2 Personal data will be retained in line with the Retention of Records Procedure (GDPR DOC 2.3) and, once its retention date is passed, it must be securely destroyed as set out in this procedure.
4.5.3 The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure (GDPR DOC 2.3), and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

4.6 Personal data must be processed in a manner that ensures the appropriate security
The Data Protection Officer will carry out a risk assessment taking into account all the circumstances of Royal School for the Deaf Derby's controlling or processing operations.
In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on Royal School for the Deaf Derby itself, and any likely reputational damage including the possible loss of customer trust.
When assessing appropriate technical measures, the Data Protection Officer will consider the following:

- Password protection
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media (GDPR DOC 11.2.7);
- Virus checking software and firewalls (GDPR-C DOC 6.2.1);
- Role-based access rights including those assigned to temporary staff (GDPR-C DOC 9.1.2);
- Encryption of devices that leave the organisations premises such as laptops (GDPR-C DOC 6.2.1);
- Security of local and wide area networks (GDPR-C DOC 6.2.1);
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to Royal School for the Deaf Derby.

When assessing appropriate organisational measures, the Data Protection Officer will consider the following:

- The appropriate training levels throughout Royal School for the Deaf Derby;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

4.7 The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)
The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.
The Royal School for the Deaf Derby will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

5. Data subjects' rights

5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.
5.1.2 To prevent processing likely to cause damage or distress.
5.1.3 To prevent processing for purposes of direct marketing.
5.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.
5.1.5 To not have significant decisions that will affect them taken solely by automated process.
5.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.
5.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
5.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
5.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
5.1.10 To object to any automated profiling that is occurring without consent.

5.2 Royal School for the Deaf Derby ensures that data subjects may exercise these rights:
5.2.1 Data subjects may make data access requests as described in Subject Access Request Procedure (GDPR DOC 2.2); this procedure also describes how Royal School for the Deaf Derby will ensure that its response to the data access request complies with the requirements of the GDPR.
5.2.2 Data subjects have the right to complain to Royal School for the Deaf Derby related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Policy

6. Consent

6.1 Royal School for the Deaf Derby understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.
6.2 Royal School for the Deaf Derby understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.
6.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.
6.4 For sensitive data, explicit written consent (Consent Procedure GDPR DOC 2.7) of data subjects must be obtained unless an alternative legitimate basis for processing exists.
6.5 In most instances, consent to process personal and sensitive data is obtained routinely by Royal School for the Deaf Derby using standard consent documents from Royal School for the Deaf Derby Portal. e.g. when a new client signs a contract, or during induction for participants on programmes.
6.6 Where Royal School for the Deaf Derby provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16

7. Security of data

7.1 All Employees/Staff are responsible for ensuring that any personal data that Royal School for the Deaf Derby holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Royal School for the Deaf Derby to receive that information and has entered into a confidentiality agreement.

7.2 All personal data should be accessible only to those who need to use it. All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Data Protection Policy
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media (GDPR-C DOC 11.2.7).

7.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of Royal School for the Deaf Derby. All Employees/Staff are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.
7.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit [written] authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with [procedure reference].
7.5 Personal data may only be deleted or disposed of in line with the Retention of Records Procedure (GDPR DOC 2.3). Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by GDPR-C DOC 11.2.7 before disposal.
7.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

8. Disclosure of data

8.1 Royal School for the Deaf Derby must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Royal School for the Deaf Derby's business.
8.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer

9. Retention and disposal of data

9.1 Royal School for the Deaf Derby shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.
9.2 Royal School for the Deaf Derby may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.
9.3 The retention period for each category of personal data will be set out in the Retention of Records Procedure (GDPR DOC 2.3) along with the criteria used to determine this period including any statutory obligations Royal School for the Deaf Derby has to retain the data.
9.4 Royal School for the Deaf Derby's data retention and data disposal procedures (Storage Removal Procedure GDPR-C DOC 11.2.7) will apply in all cases.
9.5 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure (GDPR-C DOC 11.2.7).

10. Data transfers

10.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".
The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

10.1.1 An adequacy decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required. Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.
A list of countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

10.1.2 Privacy Shield

If Royal School for the Deaf Derby wishes to transfer personal data from the EU to an organisation in the United States, it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.
Assessment of adequacy by the data controller
In making an assessment of adequacy, the UK based exporting controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

10.1.3 Binding corporate rules

Royal School for the Deaf Derby may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that Royal School for the Deaf Derby is seeking to rely upon.

10.1.4 Model contract clauses

Royal School for the Deaf Derby may adopt approved model contract clauses for the transfer of data outside of the EEA. If Royal School for the Deaf Derby adopts one of the model contract clauses there is an automatic recognition of adequacy.

10.1.5 Exceptions

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

11. Information asset register/data inventory

11.1 Royal School for the Deaf Derby has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. Royal School for the Deaf Derby's data inventory and data flow determines (GDPR DOC 2.4):

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Royal School for the Deaf Derby throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

11.2 Royal School for the Deaf Derby is aware of any risks associated with the processing of particular types of personal data.

11.2.1 Royal School for the Deaf Derby assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) (DPIA Procedure GDPR DOC 2.4) are carried out in relation to the processing of personal data by Royal School for the Deaf Derby, and in relation to processing undertaken by other organisations on behalf of Royal School for the Deaf Derby.

11.2.2 Royal School for the Deaf Derby shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

11.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Royal School for the Deaf Derby shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

11.2.4 Where, as a result of a DPIA it is clear that Royal School for the Deaf Derby is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Royal School for the Deaf Derby may proceed must be escalated for review to the Data Protection Officer

11.2.5 The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

11.2.6 Appropriate controls will be selected Annex A of ISO 27001, ISO 27017, ISO 27018 and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Royal School for the Deaf Derby's documented risk acceptance criteria and the requirements of the GDPR.

See also

Data Protection Policy
Data protection Act 2018
CCTV Policy

Appendix 1

Subject Access Request Procedure

1. Scope

All personal data processed by Royal School for the Deaf Derby is within the scope of this procedure.

Data subjects are entitled to obtain:

- Confirmation as to whether Royal School for the Deaf Derby is processing any personal data about that individual;
- Access to their personal data;
- Any related information;

2. Responsibilities

2.1 The Data Protection Officer is responsible for the application and effective working of this procedure, and for reporting to the information owner, which is the Headteacher on Subject Access Requests (SARs).

2.2 The Data Protection Officer is responsible for handling all SARs.

3. Procedure

3.1 Subject Access Requests are made using the Subject Access Request Record (GDPR REC 4.2).

3.2 The data subject provides Royal School for the Deaf Derby with evidence of their identity, in the form of [a current passport or driving license and the signature on the identity must be cross-checked to that on the application form GDPR REC 4.2.

3.3 The data subject specifies to Royal School for the Deaf Derby specific set of data held by Royal School for the Deaf Derby on their subject access request (SAR). The data subject can request all data held on them.

3.4 Royal School for the Deaf Derby records the date that the identification checks were conducted and the specification of the data sought.

3.5 Royal School for the Deaf Derby provides the requested information to the data subject within one month from this recorded date. There are no circumstances in which an extension to that one month will be provided, and failure to provide the requested information within that one month is a breach of the GDPR.

3.6 Once received, the subject access request (SAR) application is immediately forwarded to the Data Protection Officer, who will ensure that the requested data is collected within the specified time frame in clause 3.4 above.

Collection entails:

3.6.1 Collecting the data specified by the data subject, or

3.6.2 Searching all databases and all relevant filing systems (manual files) in Royal School for the Deaf Derby, including all back up and archived files (computerised or manual) and all email folders and archives. The Data Protection Officer maintains a data map that identifies where all data in Royal School for the Deaf Derby is stored.

3.7 The Data Protection Officer maintains a record of requests for data and of its receipt, including dates.

3.8 The Data Protection Officer reviews subject access requests from a child. Before responding to a SAR of the child data subject the Data Protection Officer considers their ability to making the request by adequately explaining any implications of sharing their personal data.

3.9 The Data Protection Officer reviews all documents that have been provided to identify whether any third parties are present in it, and either removes the identifying third party information from the documentation or obtains written consent from the third party for their identity to be revealed.

3.10 If any of the requested data is being held or processed under one of the following exemptions, it does not have to be provided:

- National security
- Crime and taxation
- Health
- Education

- Social Work
- Regulatory activity
- Journalism, literature and art
- Research history, and statistics
- Publicly available information
- Corporate finance
- Examination marks
- Examinations scripts
- Domestic processing
- Confidential references
- Judicial appointments, honours and dignities
- Crown of ministerial appointments
- Management forecasts
- Negotiations
- Legal advice and proceedings
- Self-incrimination
- Human fertilization and embryology
- Adoption records
- Special educational needs
- Parental records and reports

3.11 In the event that a data subject requests Royal School for the Deaf Derby to provide them with the personal data stored by the controller/processor, then Royal School for the Deaf Derby will provide the data subject with the requested information in electronic format, unless otherwise specified. All of the items provided to the data subject are listed on the GDPR Records, that shows the data subject's name and the date on which the information is delivered to Headteacher the data subject.

3.12 In the event that a data subject requests what personal data is being processed then Royal School for the Deaf Derby provides the data subject with the following information:

3.12.1 Purpose of the processing

3.12.2 Categories of personal data

3.12.3 Recipient(s) of the information, including recipients in third countries or international organisations

3.12.4 How long the personal data will be stored

3.12.5 The data subject's right to request rectification or erasure, restriction or objection, relative to their personal data being processed.

3.12.5.1 Royal School for the Deaf Derby removes personal data from systems and processing operations as soon as a request for erasure has been submitted by the data subject.

3.12.5.2 Royal School for the Deaf Derby contacts and communicates with other organisations, where the personal data of the data subject is being processed, to cease processing information at the request of the data subject.

3.12.5.3 Royal School for the Deaf Derby takes appropriate measures, without undue delay in the event that the data subject has: withdrawn consent (GDPR-REC 4.6A); objects to the processing of their personal data in whole or part; no longer under legal obligation and/or has been unlawfully processed.

3.12.6 Inform the data subject of their right to lodge a complaint with the supervisory authority and a method to do so (Complaints Procedure GDPR DOC 2.9).

3.12.7 Information on the source of the personal data if it has not been collected from the data subject.

3.12.8 Inform the data subject of any automated decision-making.

3.12.9 If and where personal data has been transferred and information on any safeguards in place.

Appendix 2

Retention of Records

1. Scope

All Royal School for the Deaf Derby's records, whether analogue or digital, are subject to the retention requirements of this procedure.

2. Responsibilities

2.1 The following roles are responsible for retention of these records because they are the information asset owners.

2.2 Asset owners are/responsible for ensuring that all personal data is collected, retained and destroyed in line with the requirements of the GDPR.

2.3 The Finance Director (CFO) is responsible for retention of financial (accounting, tax) and related records.

2.4 The Head of HR is responsible for retention of all HR records.

2.5 The Health and Safety Officer is responsible for retention of all Health and Safety records.

2.6 The Company Secretary is responsible for retention of all other statutory and regulatory records.

2.7 The Data Protection Officer is responsible for storage of data in line with this procedure.

2.8 The Manager/Executive (generic/line) is responsible for ensuring that retained records are included in business continuity and disaster recovery plans.

3. Procedure

3.1 The required retention periods, by record type, are recorded in (Retention of Records – GDPR REC 4.9) under the following categories:

3.1.1 Record type
3.1.2 Retention period
3.1.3 Retention period to start from (at creation, submission, payment, etc.)
3.1.4 Retention justification
3.1.5 Record medium
3.1.6 Disposal method

3.2 Each data asset that is stored is marked, with the name of the record, the record type, the original owner of the data, the information classification (Information Classification Procedure GDPR-C DOC 8.2), the data of storage, the required retention period, the planned date of destruction, and any special information (e.g. in relation to cryptographic keys).

3.3 Cryptographic keys, which are required for records are retained.

3.4 For all storage media (electronic and hard copy records), Royal School for the Deaf Derby retains the means to access that data.

3.5 For all electronic storage media, Royal School for the Deaf Derby does not exceed 90% of the manufacturer's recommended storage life. This is recorded in the Log of Information Assets for Disposal (GDPR-C REC 11.2.7). When the maximum of 90% of expected life is reached, the stored data is copied onto new storage media.

3.6 The procedure for accessing stored data is detailed in Access Control Rules and Rights for Users/User Group. Procedures will be followed to allow access to ensure records are protected from loss, destruction or falsification during this process.

3.7 The Data Protection Officer Headteacher are responsible for destroying data once it has reached the end of the retention period as specified in Retention and Disposal Schedule (GDPR REC 4.9). Destruction must be completed within 30 days of the planned retention period.

3.8 Portable/removable storage media are destroyed in line with GDPR-C DOC 11.2.7.

Appendix 3

Data Inventory

1. Scope

The consent of the data subject is one of the conditions for the processing of his or her personal data and is within the scope of this procedure. Royal School for the Deaf Derby needs to obtain consent when no other lawful basis applies.

Consent of the data subject is defined by the GDPR as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

Explicit consent is required for the processing of sensitive personal data. Specific conditions apply to the validity of consent given by children in relation to information society services, with requirements to obtain and verify parental consent below certain age limits.

2. Responsibilities

2.1 As a data controller, Royal School for the Deaf Derby is responsible under the GDPR for obtaining consent from the data subject under advisement from Data Protection Officer

3. Consent procedure

3.1 Royal School for the Deaf Derby provides a clear privacy notice wherever personal data is collected (GDPR REC 4.1) to ensure that consent is informed and that the data subject is informed of their rights in relation to their personal data.

3.2 Royal School for the Deaf Derby demonstrates data subject(s) consent to the processing of his or her personal data or explicit consent for sensitive personal data (GDPR REC 4.6 – Data Subject Consent Form).

3.3 Royal School for the Deaf Derby demonstrates data subject(s) consent to the processing of his or her personal data for one or more specific purposes (GDPR REC 4.6 – Data Subject Consent Form).

3.4 Royal School for the Deaf Derby demonstrates data subject(s) consent is clearly distinguishable from any other matter relating to the data subject (if recorded in paper / electronic file format use GDPR REC 4.6 – Data Subject Consent Form, or email then attach the email to the form).

3.5 Royal School for the Deaf Derby demonstrates data subject(s) consent is intelligible and accessible using clear and plain language.

3.6 Royal School for the Deaf Derby demonstrates data subject(s) are informed of their right to withdraw consent before giving consent (GDPR DOC 2.7A - Right to withdraw Consent Procedure).

3.7 Royal School for the Deaf Derby demonstrates processing of data is limited to that stated in the contract, bound by the explicit consent given by the data subject.

4. Child consent procedure

4.1 Where processing relates to a child under 16 years old, Royal School for the Deaf Derby demonstrates that consent has been provided by the person who is the holder of parental responsibility over the child (GDPR REC 4.7), in instances where Royal School for the Deaf Derby offers services online targeting children.

4.2 The Royal School for the Deaf Derby demonstrates reasonable efforts have been made to verify the age of the child and establish the authenticity of the parental responsibility taking into consideration available technology.

Appendix 4

Consent Procedure

5. Scope

The consent of the data subject is one of the conditions for the processing of his or her personal data and is within the scope of this procedure. Royal School for the Deaf Derby needs to obtain consent when no other lawful basis applies.

Consent of the data subject is defined by the GDPR as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

Explicit consent is required for the processing of sensitive personal data. Specific conditions apply to the validity of consent given by children in relation to information society services, with requirements to obtain and verify parental consent below certain age limits.

6. Responsibilities

6.1 As a data controller, Royal School for the Deaf Derby is responsible under the GDPR for obtaining consent from the data subject under advisement from Data Protection Officer

7. Consent procedure

7.1 Royal School for the Deaf Derby provides a clear privacy notice wherever personal data is collected (GDPR REC 4.1) to ensure that consent is informed and that the data subject is informed of their rights in relation to their personal data.

7.2 Royal School for the Deaf Derby demonstrates data subject(s) consent to the processing of his or her personal data or explicit consent for sensitive personal data (GDPR REC 4.6 – Data Subject Consent Form).

7.3 Royal School for the Deaf Derby demonstrates data subject(s) consent to the processing of his or her personal data for one or more specific purposes (GDPR REC 4.6 – Data Subject Consent Form).

7.4 Royal School for the Deaf Derby demonstrates data subject(s) consent is clearly distinguishable from any other matter relating to the data subject (if recorded in paper / electronic file format use GDPR REC 4.6 – Data Subject Consent Form, or email then attach the email to the form).

7.5 Royal School for the Deaf Derby demonstrates data subject(s) consent is intelligible and accessible using clear and plain language.

7.6 Royal School for the Deaf Derby demonstrates data subject(s) are informed of their right to withdraw consent before giving consent (GDPR DOC 2.7A - Right to withdraw Consent Procedure).

7.7 Royal School for the Deaf Derby demonstrates processing of data is limited to that stated in the contract, bound by the explicit consent given by the data subject.

8. Child consent procedure

8.1 Where processing relates to a child under 16 years old, Royal School for the Deaf Derby demonstrates that consent has been provided by the person who is the holder of parental responsibility over the child (GDPR REC 4.7), in instances where Royal School for the Deaf Derby offers services online targeting children.

8.2 The Royal School for the Deaf Derby demonstrates reasonable efforts have been made to verify the age of the child and establish the authenticity of the parental responsibility taking into consideration available technology.

Royal School for the Deaf Derby

Appendix 5
PIMS and GDPR Objectives Record

Purpose
Record Royal School for the Deaf Derby objectives for the implementation of PIMS and GDPR.

Date	Objective	Document reference	Responsibility	Due date

The Data Protection Officer is the owner of this document and is responsible for ensuring that it is maintained.

This document was issued by the Board of Governors and is issued on a version-controlled basis.

Signature:

Date:

Appendix 6

Security of local and wide area networks

1. Scope[1]

All users of the Royal School for the Deaf Derby's wireless notebook computers and other mobile devices are within the scope of this procedure.

2. Responsibilities

2.1 The Head of IT (CIO) is responsible for specifying and/or providing the firewalls, anti-malware software, automatic updating, connectivity and backup facilities required under this procedure.

2.2 The Head of HR is responsible for user training.

2.3 All users have specific responsibilities in terms of their User Agreements.

3. Procedure [ISO 27002 Clause 6.2.1]

3.1 Royal School for the Deaf Derby 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.

3.2 Royal School for the Deaf Derby 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.

3.3 Royal School for the Deaf Derby requires notebook computers that carry personal data, or are able to connect to systems that store or process personal data, use full-disk encryption. Royal School for the Deaf Derby's full-disk encryption solution is Deslock.

3.4 Royal School for the Deaf Derby 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.

3.5 Royal School for the Deaf Derby 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.

3.6 Royal School for the Deaf Derby requires (in the User Agreement) that notebook computers are backed up in line with corporate specification.

3.7 Royal School for the Deaf Derby requires users of notebook computers to carry with them at all times the chargers and spare batteries specified in the User Agreement.

3.8 Royal School for the Deaf Derby 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.

3.9 Royal School for the Deaf Derby requires users, 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.

3.10 Royal School for the Deaf Derby carries out regular and ad hoc audits of all notebook computers to ensure that they are configured in compliance with this procedure.

3.11 Royal School for the Deaf Derby 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.

3.12 Work instruction ISMS DOC sets out how the corporate requirements set out in Clause 3.1 and 3.4 above are enforced.

3.13 WI ISMS DOC sets out how the VPN or other connectivity solution is to be operated.

3.14 WI ISMS DOC sets out how e-mails are to be encrypted when sent from mobile devices.

[1] **Chapter 21** of IT Governance: An International Guide to Data Security and ISO27001/ISO27002 deals with mobile computing. This template will need to be expanded to take into account mobile phones, Blackberries, PDAs and any other mobile devices, and adjusted to reflect different decisions on connectivity.

Appendix 7

Secure Disposal of Storage Media Procedure

1. Scope

Royal School for the Deaf Derby 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.

2. Responsibilities

2.1 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.

2.2 All owners of removable storage media are responsible for ensuring that these media are disposed of in line with this procedure.

3. Procedure [ISO27002 Clauses 8.3.2 11.2.7]

3.1 Hard disks must be cleared of all software and all organisational confidential and restricted information prior to disposal or reuse, as set out in Clause 3.5 and 3.6, below.

3.1.1 In the event that hard disks/media contain personal data, and it cannot be removed, then:

3.1.1.1 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.

3.1.1.2 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.

3.2 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.

3.3 Hard disks are cleaned and a WEEE and hardware destruction certification is issued.

3.4 Devices containing confidential information dependent on a risk assessment are destroyed prior to disposal and are never reused.

3.5 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.

3.6 Portable or removable storage media of any description are destroyed prior to disposal.

3.7 All media are disposed of in line with regulations on disposal of computer equipment, through Royal School for the Deaf Derby's approved contractor.

3.8 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 8
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: Data controller: Royal School for the Deaf Derby Governing Body. Contact: Nicola Hardy, Clerk to the Governors at, nicola.hardy@rsdd.org.uk
Data protection officer: Bruno Gambini, Campus Resources Manager, Royal School for the Deaf Derby Email: bruno.gambini@rsdd.org.uk Voice & SMS: 07500 878592

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; 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 Bruno Gambini, campus Resources manager at, bruno.gambini@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 contact details of the 4.4, 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 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

Royal School for the Deaf Derby

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, Royal School for the Deaf Derby, 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.
To view our policy please request a copy of policy GDPR Doc 2.4 from the school office.

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, Royal School for the Deaf Derby are the 'data controller' for the purposes of data protection law.

Our data protection officer is Bruno Gambini bruno.gambini@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.

Royal School for the Deaf Derby

Job Applicant Privacy Notice

Data controller: Royal School for the Deaf Derby Governing Body. Contact: Nicola Hardy, Clerk to the Governors at, nicola.hardy@rsdd.org.uk

Data protection officer: Bruno Gambini, Campus Resources Manager, Royal School for the Deaf Derby Email: bruno.gambini@rsdd.org.uk Voice & SMS: 07500 878592

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 Bruno Gambini, Campus resources manager by email at bruno.gambini@rsdd.org.uk or by voice or SMS on 07500
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.