Data Protection Policy

Audience:	REAch2 Staff Local Governing Bodies Trustees Parents and all public
Ratified:	REAch2 Trust Board September 2025
Other related policies:	Privacy Notice for Employees Privacy Notice for Parents Information Security Policy Child Protection Policy Subject Access Request (SAR) procedure DPIA procedure Data Breach procedure
Policy owner:	Claire Lockyer, Trust DPO
Review:	August 2028

At REAch2, our actions and our intentions as school leaders are guided by our Touchstones.

Policy Overview ***5***
Policy Statement 5
About This Policy 5
Definition of Data Protection Terms 5
Data Protection Officer 6
Policy In Detail ***6***
Our Data Protection Commitments 6
Data Protection Principles 6
Legal Grounds for Processing 7
Data Subjects' Rights 9
Data Protection by Design and Default 10
Data Security 10
Personal Data Breaches 11
Disclosure and Sharing of Personal Information 11
Data Processors 12
Images and Videos 12
Changes to this Policy 13
Policy Review ***13***
Appendices ***13***
Definitions 13
Special Category Data Policy ***15***
Introduction 15
Definitions 16
Workforce Special Category Data 16
Pupil and Parent Special Category Data 17
Compliance with the Data Protection Principles 18
Lawful, Fair and Transparent 18
Purpose Limitation 21
Data Minimisation 21
Accuracy 21
Storage Limitation 21
Security, Integrity and Accountability 22
Accountability 22
Policies on Retention and Deletion 22

Review 23

Policy Overview

Policy Statement

1 During the course of our activities as a Trust, we will collect, store and **process personal data** about our pupils, **workforce**, parents and others.

2 We are committed to the protection of all **personal data a**nd **special category personal data** and this policy sets out how we comply with relevant legislation. Breaches of this policy can result in the risk of real harm to individuals, action for damages, loss of trust and reputational harm as well as regulatory penalties, including fines.

3 All **data users** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action. Individuals may be prosecuted for committing offences under sections 170-173 of the Data Protection Act 2018.

About This Policy

4 The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the UK General Data Protection Regulation ("**GDPR**"), the Data Protection Act 2018, and other regulations (together "**data protection legislation"**).

5 This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.

6 This policy does not form part of any employee's contract of employment and may be amended at any time.

7 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

Definition of Data Protection Terms

All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the Annex to this policy.

Data Protection Officer

1 As a Trust, we are required to appoint a Data Protection Officer ("**DPO**"). Our DPO is Claire Lockyer, and they can be contacted at dataprotectionofficer@reach2.org.

2 The DPO is responsible for informing and advising the Trust about **data protection legislation**, ensuring compliance with the law and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

3 The DPO is also the central point of contact for all data subjects, **the Information Commissioner's Office** ("**ICO**") and others in relation to matters of data protection.

Policy In Detail

Our Data Protection Commitments

1 We are dedicated to ensuring that personal data is processed in alignment with the legal principles of data protection;
2 We implement a strategy focused on "Data Protection by Design and Default";
3 We can prove our adherence to data protection legislation;
4 Data subjects are well-informed about how and why we use their data, and they can exercise their rights regarding their data;
5 We share personal data only when it is fair and lawful, ensuring that any data sharing is conducted securely;
6 We handle and report all personal data breaches, including minor ones, effectively to mitigate any potential risks and to improve our practices.

Data Protection Principles

1 Anyone processing personal data must comply with the data protection principles. We will comply with these principles in relation to any processing of personal data by the Trust.
2 The principles provide that personal data must be:
   a. Processed fairly and lawfully and transparently in relation to the data subject. This means that we only use personal data with respect for the individual who it relates to, in line with the legal grounds for processing and we inform data subjects how their data is processed including, among other ways, in our privacy notices;
   b. Processed for specified purposes and in a way which is not incompatible with those purposes. This means that if we collect data for one purpose and then need to use it for another reason we will ensure that new purpose is compatible with the original reason for processing;

c. Adequate, relevant and not excessive for the purpose. This means that we will collect enough information to achieve our aim, whilst minimising that collection to what is genuinely required;
d. Accurate and up to date. This means that we will try to ensure that data is accurate when we collect it, and kept up-to-date over time;
e. Not kept for any longer than is necessary for the purpose. This means that we only keep personal data for as long as it is necessary and we comply with our [Data Retention Policy]; and
f. Processed securely using appropriate technical and organisational measures. Our measures include: technical safeguards like security of ICT systems, control over ICT access, the use of pseudonyms, and encryption; as well as organisational safeguards including plans for business continuity, securing our premises and data physically, implementing policies and procedures, conducting regular training, and carrying out audits and evaluations of operational measures and strategic oversight of compliance.

3 Personal Data must also:

a. be processed in line with data subjects' rights;
b. not be transferred to people or organisations situated in other countries without adequate protection.

Legal Grounds for Processing

8 For **personal data** to be **processed** lawfully, it must be **processed** based on one of the legal grounds set out in the **data protection legislation**. We will normally **process personal data** under the following legal grounds:

8.1 where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;

8.2 where the **processing** is necessary to comply with a legal obligation that we are subject to;

8.3 where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest; and

8.4 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data**.

9 When **special category personal data is** being processed then an additional legal ground must apply to that **processing**. We understand that for certain types of **processing** of this data we must have and comply with an appropriate policy document (available as Annex 2). We will normally only process **special category personal data** under following legal grounds:

9.1 where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;

10 where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;

10.1 where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and

10.2 where none of the above apply then we will seek the explicit consent of the **data subject** to the **processing** of their **special category personal data**.

11 We will inform **data subjects** of the above matters by way of appropriate **privacy notices** which shall be provided to them when we collect the data or as soon as possible thereafter unless we have already provided this information such as at the time when a pupil joins us.

12 If any **data user** is in doubt as to the legal ground for processing, then they must contact the DPO before doing so.

Vital Interests

13 There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not able to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

14 Where none of the other bases for **processing** set out above apply then the Trust must seek the consent of the **data subject** before **processing** any personal data for any purpose.

15 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

16 When pupils and/or our **workforce** join the Trust, a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

17 In relation to all pupils, due to their age, we will seek consent from an individual with parental responsibility for that pupil.

18 If consent is required for any other **processing** of **personal data** of any **data subject** then the form of this consent must:

18.1 Inform the **data subject** of exactly what we intend to do with their **personal data**;

18.2 Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and

18.3 Inform the **data subject** of how they can withdraw their consent.

19 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent. We will ensure that it will be as easy for the **data subject** to withdraw their consent as it was to give it.

20 The DPO must always be consulted in relation to any consent form before consent is obtained.

21 A record must always be kept of any consent, including how it was obtained and when.

Data Subjects' Rights

1 In addition to the right to be informed and the right to withdraw consent, we will **process** all **personal data** in line with **data subjects**' rights, in particular their right to:

1.1 request access to any **personal data** we hold about them;

1.2 object to the **processing** of their **personal data**, including the right to object to direct marketing;

1.3 have inaccurate or incomplete **personal data** about them rectified;

1.4 restrict processing of their **personal data**;

1.5 have **personal data** we hold about them erased; and

1.6 object to the making of decisions about them by automated means.

2 The rights available to **data subjects** will depend on the lawful basis for **processing**, for example, where **personal data** is **processed** under the lawful basis of public task, then the **data subject** cannot withdraw consent for such **processing**, but they can exercise the right of objection.

3 Except for the right to object to direct marketing, other rights requests in an education or employment context can be complex. We will comply with our obligations under **data protection laws** and the guidance given by the **ICO** in respect of individuals seeking to exercise their rights.

4 We will consider **data subject** requests and provide a response within one month, except if we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary, then we will inform the **data subject** within one month of their request that this is the case.

5 Where we are unable to grant **data subjects** any requests made as part of their rights, for example, where we are unable to delete data as we are required to retain it in relation to any claim or legal proceedings, we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the **ICO** at the time that we inform them of our decision in relation to their request.

6 The DPO must be consulted in relation to any **data subject** rights requests.

The Right of Access to Personal Data

7 **Data subjects** may request access to **personal data** we hold about them. Such requests will be considered in line with the Trust Subject Access Request Procedure available from the Trust website.

Data Protection by Design and Default

1 The Trust will consider and comply with the requirements of **data protection legislation** in relation to all its activities whenever these involve the use of **personal data**, in accordance with the principles of data protection by design and default.

2 In certain circumstances the law requires us to carry out detailed assessments of proposed processing in a **Data Protection Impact Assessment** ("**DPIA**"). This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or there is a change in our existing ways of working.

3 The Trust will complete a **DPIA** for such proposed **processing** and has a template document which ensures that all relevant matters are considered. We may also carry out **DPIAs** where one is not legally required, as a matter of good practice.

4 The DPO should always be consulted as to whether a **DPIA** is required, and if so how to undertake that assessment.

We carry out and review **DPIAs** in accordance with our DPIA procedure available internally on the Data Protection area of the REAchIn Intranet site or by request from dataprotectionofficer@reach2.org.

Data Security

1 We will take appropriate security measures against unlawful or unauthorised **processing** of **personal data**, and against the accidental loss of, or damage to, **personal data**.

2 We will put in place procedures and technologies to maintain the security of all **personal data** from the point of collection to the point of destruction.

3 Security procedures include:

3.1 Entry controls. Any stranger seen in entry-controlled areas should be reported to a member of SLT (if in school) or to any member of staff if in Central premises.

3.2 Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (**Personal data** is always considered confidential).

3.3 Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with **ICO** guidance on the disposal of IT assets.

3.4 Equipment. **Data users** must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

3.5 Working away from the school premises – paper documents. Please see Information Security Policy, available internally on REAchIn intranet or by requests from dataprotectionofficer@reach2.org.

3.6 Working away from the school premises – electronic working. Please see Information Security Policy, available internally on REAchIn intranet or on request from dataprotectionofficer@reach2.org

3.7 Document printing. Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

Personal Data Breaches

1 The Trust recognises that a breach of **personal data** could happen, despite our policies, procedures and measures in place to protect **personal data**, and we will respond to any breach as quickly as possible in order to minimise any risks or potential harm to individuals.

2 The Trust Personal Data Breach Procedure supports this policy and must be followed in relation to any actual or suspected breach of **personal data**. The Trust data breach procedure is available internally on REAchIn intranet or on request from dataprotectionofficer@reach2.org.

Disclosure and Sharing of Personal Information

1 We may share **personal data** that we hold about **data subjects** with other organisations. Such organisations include the Department for Education, and/or Education and Skills Funding Agency "**ESFA**", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

2 The Trust will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

3 Where necessary we will enter into data sharing agreements to help facilitate the safe sharing of **personal data**.

4 In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

Data Processors

1 We contract with various organisations who provide services to the Trust. These include people, companies, and systems that process personal data on our behalf and under our instruction.

2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

3 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of the Trust. The Trust will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

4 Contracts with **data processors** will comply with **data protection legislation** and contain explicit obligations on the **data processor** to ensure compliance with the **data protection legislation**, and compliance with the rights of **data subjects**.

Images and Videos

1 Parents and others attending Trust events are allowed to take photographs and videos of those events for personal and domestic purposes. For example, parents can take video recordings of a school performance involving their child. The Trust does not prohibit this as a matter of policy although all Trust schools are able to requests filming is not made. This policy does not override decisions of individual schools with regard to filming and such decisions are taken with the safety of all our children and staff as paramount.

2 The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.

3 The Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

4 Whenever a pupil begins their attendance at the Trust their parent will be asked to complete a consent form in relation to the use of images and videos of that pupil. Images and videos of pupils may be required for safeguarding, assessment and learning purposes and we will not seek consent for the taking and use of these images. However, as a Trust we want to celebrate the achievements

of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of parents before allowing the use of images or videos of pupils for such purposes.

Changes to this Policy

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

Policy Review

The Data Protection Policy will be reviewed **every 3 years** or sooner, taking into account any legislative changes.

Any changes made to this policy will be communicated to all relevant stakeholders.

Appendices

Definitions

Term	Definition
Data	is information, which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal Data	means any information relating to an identified or identifiable natural person (a 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.

Term	Definition
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data Users	are those of our workforce (including Governors, temporary or agency staff and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Data Protection Impact Assessment (DPIA)	a tool to help identify how to comply with data protection obligations and protect individuals' rights as set out in Article 35 of the UK GDPR. The ICO also has guidance on DPIAs on their website at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/
Data Protection Legislation	Means all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR; the Data Protection Act 2018 (DPA 2018) (and regulations made thereunder); and the Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to the use of personal data.
Information Commissioner's Office (ICO)	in the UK, the Information Commissioner's Office (ICO) is the data protection regulator. The website of the ICO is at www.ico.org.uk.
Privacy notices	where we collect information either directly or indirectly from data subjects, we provide them with a statement of fair processing, referred to as a privacy notice. This notice will contain information about: our identity and contact details as Data Controller and those of the DPO; the purpose or purposes and legal basis for which we intend to process that personal data; the types of third parties, if any, with which we will share or to which

Term	Definition
	we will disclose that personal data; whether the personal data will be transferred outside the UK and if so the safeguards in place; the period for which their personal data will be stored, by reference to our Data Retention Policy; the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making; and the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data 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. Processing also includes transferring personal data to third parties.
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.
Workforce	Includes, any individual employed by the Trust such as staff and those who volunteer in any capacity including Governors and/or Trustees/Members/parent helpers.

Special Category Data Policy

Introduction

1 This policy is intended to clearly set out the requirements of the UK General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018 (**DPA 2018**) which are relevant to Trust's use of sensitive personal data, known as "**special category data**".

2 It applies to all **special category data** which is processed by the Trust about our **workforce** and also the **special category data** of pupils and parents which is also processed on behalf of the Trust.

3 This policy has been drafted to meet the requirements of the DPA 2018 that an appropriate policy document be put in place where **processing special category data** and **criminal convictions data** in certain circumstances.

Definitions

4 For the purposes of this policy:

4.1 **Criminal convictions data** means any personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings (any the absence of any criminal record).

4.2 **Information Commissioner's Office (ICO)** means in the UK, the Information Commissioner's Office (ICO) is the data protection regulator. The website of the ICO is at www.ico.org.uk.

4.3 **Personal data** means any information that relates to an identifiable, living individual.

4.4 **Privacy notice** means the privacy information we provide where we collect information either directly or indirectly from data subjects, which is referred to as a privacy notice. This notice will contain information about: our identity and contact details as data controller and those of the DPO; the purpose or purposes and legal basis for which we intend to process that personal data; the types of third parties, if any, with which we will share or to which we will disclose that personal data; whether the personal data will be transferred outside the UK and if so the safeguards in place; the period for which their personal data will be stored, by reference to our Data Retention Policy; the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making; and the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

4.5 **Process, processing or processed** means any operation performed on personal data. This includes collecting, recording, organising, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating or otherwise making available or destroying personal data.

4.6 **Special category data** means personal data revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sex life, sexual orientation, biometric or genetic data.

4.7 **Workforce** means any individual employed by the Trust such as staff and those who volunteer in any capacity including Governors and/or Trustees/Members/parent helpers.

Workforce Special Category Data

5 The UK GDPR and the DPA 2018 set out strict rules about the way in which **special category data** and **criminal convictions data** are collected, accessed, used and disclosed. Some of the Schedule 1 conditions in the DPA 2018 for **processing special category data** require us to have an appropriate policy document in place, setting out and explaining our procedures for securing compliance with the principles set out in Article 5 UK GDPR and our policies regarding the retention and erasure of **special category data**. This policy explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

6 We **process** the **special category data** and **criminal convictions data** of our **workforce** under the UK GDPR under the following lawful bases, depending on the specific purpose for **processing**:

6.1 Article 9(2)(a) UK GDPR – explicit consent

6.2 Article 9(2)(b) UK GDPR – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Trust or an individual in connection with employment, social security or social protection.

6.3 Article 9(2)(c) UK GDPR – where processing is necessary to protect the vital interests of an individual.

6.4 Article 9(2)(g) UK GDPR – for reasons of substantial public interest.

6.5 Article 9(2)(f) UK GDPR – for the establishment, exercise or defence of legal claims.

7 We process special category data and criminal conviction data of our workforce for the following purposes:

a. assessing an individual's fitness to work

b. assessing an individual's suitability to work within an education setting

c. complying with health and safety obligations

d. complying with our legal obligations to safeguard children and young people in accordance with Keeping Children Safe in Education statutory guidance

e. complying with equality legislation

f. checking applicants' and employees' right to work in the UK

g. verifying that candidates are suitable for employment or continued employment.

Pupil and Parent Special Category Data

8 We process the **special category data** and **criminal convictions data** of pupils and parents under the UK GDPR on the following legal bases, depending on the specific purpose for **processing**:

8.1 Article 9(2)(a) UK GDPR – explicit consent

8.2 Article 9(2)(b) UK GDPR – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Trust or an individual in connection with employment, social security or social protection.

8.3 Article 9(2)(c) UK GDPR – where processing is necessary to protect the vital interests of an individual.

8.4 Article 9(2)(g) UK GDPR – for reasons of substantial public interest.

8.5 Article 9(2)(f) UK GDPR – for the establishment, exercise or defence of legal claims.

9 We process special category data and criminal conviction data of pupils and parents for the following purposes:

9.1 ensuring medical needs are met

9.2 making reasonable adjustments for the provision of learning

9.3 monitoring equality of opportunity

9.4 complying with our legal obligations to safeguard children and young people in accordance with Keeping Children Safe in Education statutory guidance

9.5 complying with equality legislation

9.6 supporting pupils with special educational needs

Compliance with the Data Protection Principles

10 The UK GDPR requires **personal data** to be **processed** in accordance with the six principles set out in Article 5(1) UK GDPR. Article 5(2) UK GDPR requires organisations to be able to demonstrate compliance with Article 5(1) UK GDPR.

11 We comply with the principles relating to **processing** of **special category data** and **criminal convictions data** set out in the UK GDPR which require personal data to be:

Lawful, Fair and Transparent

12 **Personal data** must be **processed** lawfully, fairly and in a transparent manner in relation to the individual.

13 We will only **process personal data** fairly and lawfully and for specified purposes. We will only **process special category data** if we have a legal ground for **processing** as set out in the UK GDPR and one of the specific processing conditions relating to **special category data** in the DPA 2018.

14 When collecting **special category data** and **criminal convictions data**, we will provide individuals with a **privacy notice** setting out all the information required by the UK GDPR in a **privacy notice** which is concise, transparent, intelligible, easily accessible and in clear plain language which can be easily understood.

15 We have identified and documented the legal grounds and specific **processing** conditions for **processing** special category data as follows:

Workforce

Special Category Data	Lawful Basis for Processing Personal Data	Lawful Basis for Processing Special Category Data	Processing Condition for Special Category Data
Health Information	Compliance with a legal obligation (*Article 6(1)(c) UK GDPR*) or necessary for the performance of a contract (Article 6(1)(b) UK GDPR).	Compliance with employment obligations (*Article 9(2)(b) UK GDPR)*	Compliance with employment law (*Paragraph 1(1)(a), Schedule 1, DPA 2018*.)
Racial or ethnic origin, religious and sexuality data	Compliance with a legal obligation (*Article 6(1)(c) UK GDPR*)	Compliance with employment obligations (*Article 9(2)(b) UK GDPR*)	Compliance with employment law (*Paragraph 1(1)(a), Schedule 1, DPA 2018*.)
Equal opportunities data	Necessary for the purposes of our legitimate interests (*Article 6(1)(f) UK GDPR*)	Necessary for reasons of substantial public interest (*Article 9(2)(g)*)	Necessary for monitoring equality and diversity (*Paragraph 8(1)(b), Schedule 1, DPA 2018*.)

Special Category Data	Lawful Basis for Processing Personal Data	Lawful Basis for Processing Special Category Data	Processing Condition for Special Category Data
Criminal offences data	Compliance with a legal obligation (*Article 6(1)(c) UK GDPR*)	Compliance with employment obligations (*Article 9(2)(b) UK GDPR*)	Compliance with employment law (*Paragraph 1(1)(a), Schedule 1, DPA 2018.*)

Pupils and Parents

Special Category Data	Lawful Basis for Processing Personal Data	Lawful Basis for Processing Special Category Data	Processing Condition for Special Category Data
Health Information	Compliance with a legal obligation (*Article 6(1)(c) UK GDPR*) or necessary for the performance of a contract (*Article 6(1)(b) UK GDPR*).	Compliance with employment or social protection obligations (Article 9(2)(b) UK GDPR)	Compliance with employment or social protection obligations (*Paragraph 1(1)(a), Schedule 1, DPA 2018.)*
Racial or ethnic origin, religious and sexuality data	Compliance with a legal obligation (*Article 6(1)(c) UK GDPR*)	Compliance with employment or social protection obligations (*Article 9(2)(b) UK GDPR*)	Compliance with employment or social protection obligations (*Paragraph 1(1)(a), Schedule 1, DPA 2018.*)
Equal opportunities data	Necessary for the purposes of our legitimate interests (*Article 6(1)(f) UK GDPR*)	Necessary for reasons of substantial public interest (*Article 9(2)(g))*	Necessary for monitoring equality and diversity (*Paragraph 8(1)(b), Schedule 1, DPA 2018.*)
Criminal offences data	Compliance with a legal obligation (*Article 6(1)(c) UK GDPR*)	Compliance with employment or social protection obligations (*Article 9(2)(b) UK GDPR*)	Compliance with employment or social protection obligations (*Paragraph 1(1)(a), Schedule 1, DPA 2018.*)

Purpose Limitation

16 All **personal data** must be collected only for specified, explicit and legitimate purposes. It must not be further **processed** in any manner incompatible with those purposes.

17 We will only collect **personal data** for specified purposes and will inform individuals what those purposes are in a published **privacy notice**.

Data Minimisation

18 **Personal data** shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is **processed**.

19 We will only collect or disclose the minimum **personal data** required for the purpose for which the data is collected or disclosed. We will ensure that we do not collect excessive data and that the **personal data** collected is adequate and relevant for the intended purposes.

Accuracy

20 **Personal data** must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when it is inaccurate.

21 We will ensure that the **personal data** we hold and use is accurate, complete, kept up to date and relevant to the purpose for which it is collected by us. We check the accuracy of any **personal data** at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date **personal data**.

Storage Limitation

22 We only keep **personal data** in an identifiable form for as long as necessary for the purposes for which it was collected, or where we have a legal obligation to do so. Once we no longer need **personal data** it shall be deleted or rendered permanently anonymous.

23 We maintain a [Data Retention Policy] to ensure that **personal data** is deleted after a reasonable time has elapsed for the purposes for which it was being held, unless we are legally required to retain that data for longer.

24 We will ensure individuals are informed of the period for which data is stored and how that period is determined in any applicable **privacy notice**.

Security, Integrity and Accountability

25 **Personal data** shall be **processed** in a manner that ensures appropriate security of the **personal data**, including protection against unauthorised or unlawful **processing** and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

26 We will implement and maintain reasonable and appropriate security measures against unlawful or unauthorised **processing** of **personal data** and against the accidental loss of or damage to **personal data**.

Accountability

27 We are responsible for, and able to demonstrate compliance with these principles. In particular, we shall:

27.1 Ensure that records are kept of all data processing activities, and that these are provided to the **ICO** on request.

27.2 Carry out a data protection impact assessment for any high-risk **personal data processing** to understand how processing may affect individuals and consult the **ICO** if appropriate.

27.3 Ensure that a Data Protection Officer is appointed to provide independent advice and monitoring of **personal data** handling, and that the Data Protection Officer has access to report to the highest management level.

27.4 Have internal processes to ensure that **personal data** is only collected, used or handled in a way that is compliant with the UK GDPR and the DPA 2018.

Policies on Retention and Deletion

28 We take the security of **special category data** and **criminal conviction data** very seriously. We have technical and organisational safeguards in place to protect **personal data** against unlawful or unauthorised **processing**, or accidental loss or damage. We will ensure, where **special category** and/or **criminal conviction data** is **processed** that:

28.1 The **processing** is recorded, and the record sets out where possible, a suitable time period for the safe and permanent erasure of the different categories of data in accordance with our Data Retention Policy.

28.2 Where we no longer require **special category** or **criminal conviction data** for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as possible.

28.3 Where records are destroyed, we will ensure that they are safely and permanently disposed of in accordance with our Data Retention Policy.

28.4 Individuals receive a **privacy notice** setting out how their **personal data** will be handled when we first obtain their **personal data** and this will include the period for which the **personal data** will be stored, or if that is not possible, the criteria used to determine that period. Our parents' **privacy notice** is also available on our website and our intranet for our workforce.

Review

29 This policy is reviewed every 3 years by the Data Protection Officer.