

Data Protection Policy

2025-2026

Version 1.7

Date approved by Trustees of The Harbour Schools Partnership	24th September 2025
Review Period	Annual

Contents

1	Introduction and purpose	3
	The purpose of this policy is to explain how the Trust handles personal data under the data protection legislation, and to inform employees and other individuals who process personal data on the Trust's behalf, of the Trust's expectations in this regard.	3
2	Scope	3
3	Definitions	3
4	Roles and responsibilities	4
4.1	Board of Trustees	4
4.3	Data Protection Officer	4
4.4	Employees, temporary staff, contractors, visitors	4
5	Data protection by design and by default	5
6	Data Protection Principles	5
6.1	Personal data shall be processed lawfully, fairly and in a transparent manner	5
6.2	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes	7
6.3	Personal data shall be adequate, relevant and limited to what is necessary for the purpose it was processed	7
6.4	Personal data shall be accurate and where necessary kept up to date; every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay	7
6.5	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed	7
6.6	Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.....	7
6.7	Technical security measures:	7
6.8	Organisational security measures:.....	8
7	Data subjects' rights	8
8	Personal data breaches	9
8.1	Notification to the ICO and Data Subjects	10
9	Sharing data.....	10
9.1	Sharing data with suppliers (data processors).....	11
10	Data Protection Impact Assessments.....	11
11	Records management.....	12
11.1	Record of processing activities	12
	Links to other Trust Policies.....	12
	Appendix 1 Data Protection Policy Definitions.....	16

1 Introduction and purpose

This policy sets out the Trust's commitment to handling personal data in line with the General Data Protection Regulation 2016 (UK GDPR) and the Data Protection Act 2018 (collectively referred to as the data protection legislation).

The Trust is the data controller for the personal data it processes and is registered with the Information Commissioner's Office (ICO) under registration number Z2879577. Details about this registration can be found at www.ico.org.uk

The purpose of this policy is to explain how the Trust handles personal data under the data protection legislation, and to inform employees and other individuals who process personal data on the Trust's behalf, of the Trust's expectations in this regard.

2 Scope

This policy applies to the processing of personal data held by the Trust. This includes personal data held about pupils, parents/carers, employees, temporary staff, governors, visitors and any other identifiable data subjects.

This policy should be read alongside the Trust's other policies, procedures and documentation, which refer to the handling of personal data:

- CCTV policy
- Online Safety Policy
- Personal Data Breach Handling Procedure
- Data Protection Request Handling Procedure
- Record Retention Schedule

3 Definitions

There are several terms used in the data protection legislation and in this policy, which must be understood by those who process personal data held by the Trust. These are:

- Personal data
- Special categories of personal data
- Processing
- Data subject
- Data controller
- Data processor

3.2 These terms are explained in Appendix 1.

4 Roles and responsibilities

4.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring the Trust implements this policy and continues to demonstrate compliance with the data protection legislation. This policy shall be reviewed by the Board of Trustees on an annual basis.

4.2 Headteachers

The Headteacher has day-to-day responsibility for ensuring this policy is adopted and adhered to by employees and other individuals processing personal data on the Trust's behalf.

4.3 Data Protection Officer

The Data Protection Officer (DPO) is responsible for carrying out the following tasks:

- Informing and advising the Trust of their obligations under the data protection legislation
- Monitoring compliance with data protection policies
- Raising awareness and providing training
- Carrying out audits on the Trust's processing activities
- Providing advice regarding Data Protection Impact Assessments and monitoring performance
- Co-operating with the Information Commissioner's Office
- Acting as the contact point for data subjects exercising their rights

The Trust's DPO is John Walker of PHPLaw Ltd, an external company who performs the role under a service contract. The DPO can be contacted directly at info@phplaw.co.uk and [through the schools GDPR Portal](#)

The DPO is supported in their role by a Trust employee, this person is known as the Information & Governance Lead. All enquiries, complaints, requests and suspected breaches of security, should be referred to the Data Protection Officer in the first instance through the schools GDPR portal.

The DPO reports directly to the Board of Trustees and Executive Leadership Team and shall provide regular updates on the Trust's progress and compliance with the data protection legislation.

4.4 Employees, temporary staff, contractors, visitors

All employees, temporary staff, contractors, visitors and others processing personal data on behalf of the Trust, are responsible for complying with the contents of this policy. Failure to comply with this policy may result in disciplinary action or termination of employment or service contract.

All employees, temporary staff, contractors, visitors shall remain subject to the common law duty of confidentiality when their employment or relationship with the Trust ends. This does not affect an individual's rights in relation to whistleblowing. On termination of employment, employees shall return all information and equipment to the Trust, including personal identification passes/smart cards and keys.

Unauthorised access, use, sharing or procuring of the Trust's data may constitute a criminal offence under the Data Protection Act 2018 and/or the Computer Misuse Act 1990.

Employees shall have no expectation of privacy in their use of the Trust's systems. Any correspondence, documents, records or handwritten notes created for work related purposes, may be disclosable to data subjects

or the public under the UK General Data Protection Regulation, the Freedom of Information Act 2000 or Environmental Information Regulations 2004.

5 Data protection by design and by default

The Trust is committed to ensuring that data protection considerations are at the heart of everything it does involving personal data and shall ensure that it has appropriate technical and organisational measures in place which are designed to implement the Data Protection Principles in an effective manner.

The Trust shall ensure that by default, it will only process personal data where it is necessary to do so, and appropriate safeguards are in place to protect it. This Data Protection Policy and supplementary policies, procedures and guides demonstrate how the Trust achieves their 'data protection by design and default' obligations.

6 Data Protection Principles

The UK GDPR provides a set of 6 principles which govern how the Trust handles personal data. These are set out in Article 5 of the UK GDPR. All employees, temporary staff, contractors, and other individuals processing personal data on behalf of the Trust are responsible for complying with the data protection principles:

6.1 Personal data shall be processed lawfully, fairly and in a transparent manner (*'lawfulness, fairness and transparency'*).

This means personal data shall only be processed where there is a lawful basis which allows this; we are fair to data subjects when we use or share their personal data (i.e. we must act in a way they would reasonably expect); and are transparent in how we handle personal data by describing this in our privacy notices. The Trust's privacy notices are available [here](#).

The data protection legislation lists the different lawful bases which permit the collection, use and sharing etc of personal data. These are contained in Article 6 of the UK GDPR. At least one of these legal bases must apply when processing personal data. In summary:

- The data subject has given consent.
- It is necessary for contractual purposes.
- It is necessary to comply with a legal obligation.
- It is necessary to protect someone's life.
- It is necessary to carry out a task in the public interest or exercise our official duties.
- It is necessary to pursue the Trust's legitimate interests or a third party's legitimate interests, except where such interests are overridden by the data subject, in particular, where the data subject is a child.

When 'special categories' of personal data are processed (ie data which reveals a person's racial or ethnic data; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; health data; sex life or sexual orientation), this shall only be done where a lawful basis has been identified from the list above, and one from the following list:

- The data subject has given explicit consent.
- The processing is necessary for employment, social security or social protection purposes (e.g. safeguarding individuals at risk; protection against unlawful acts; prevention against fraud).

- It is necessary to protect the data subject's life and they are physically or legally incapable of giving consent.
- The data subject has made the information public.
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- The processing is necessary for reasons of substantial public interest and are proportionate to the aim pursued.
- The processing is necessary for health or social care purposes.
- The processing is necessary for reasons of public interest in public health.
- The processing is necessary for archiving purposes in the public interest, scientific or historical research or statistical purposes.

Although consent is one of the lawful bases that can be relied upon when processing personal data or special category data, it is not appropriate to rely on this for most of the processing the Trust does. This is because there is a high standard for achieving 'valid' consent and there are potential difficulties for the Trust should the data subject later withdraw their consent to the processing. The Trust shall therefore look for alternative lawful bases to legitimise its processing where they are more appropriate, such as *'processing is necessary to carry out a task in the public interest or exercise official duties'* and *'processing is necessary for the purposes of employment, social security or social protection'*.

There are however circumstances when the Trust is required to obtain consent to process personal data, for example:

- To collect and use biometric information (eg fingerprints and facial images) to be used for identification purposes.
- To send direct marketing or fundraising information by email or text, where the data subject would not have a reasonable expectation that their data would be used in this way or has previously objected to this.
- To take and use photographs, digital or video images and displaying, publishing or sharing these in a public arena (such as on social media, on the Trust website; in the Press; in the prospectus; newsletter etc), where the data subject would not have a reasonable expectation that their images would be used in this way, or the rights of the data subject override the legitimate interests of the Trust.
- To share personal data with third parties (e.g. professionals, agencies or organisations) where the data subject has a genuine choice as to whether their data will be shared, for example when offering services which the data subject does not have to accept or agree to receive.

Where it is appropriate for the Trust to use consent as its lawful basis, it shall ensure the person providing it has positively opted-in to the proposed activity and is fully informed as to what they are consenting to and any nonobvious consequences of giving or refusing that consent.

Consent shall not be assumed as being given if no response has been received e.g. a consent form has not been returned. Where consent is being obtained for the collection or use of children's information, consent shall be obtained from a parent or guardian until the child reaches their 13th birthday. Consent shall be obtained directly from children aged 13 years and over where those children are deemed by the Trust to have sufficient maturity to make the decision themselves (except where this is not in the best interests of the child. In such cases, consent will be obtained from an adult with parental responsibility for that child).

The Trust shall ensure that where consent is obtained, there is a record of this. Where possible, consent shall be obtained in writing. All forms requesting consent shall include a statement informing the person of their right to withdraw or amend their consent, and instructions on how to do this easily.

6.2 Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (*'purpose limitation'*).

This means the Trust shall only collect and use personal data for the reasons specified or described in its privacy notices and shall not process this data in any way which could be considered incompatible with those purposes, in other words, using the data for a different or unexpected purpose.

6.3 Personal data shall be adequate, relevant and limited to what is necessary for the purpose it was processed (*'data minimisation'*).

This means the Trust shall ensure that any personal data collected, used or shared etc. is fit for purpose, relevant and not excessive or disproportionate for the purpose it was intended.

6.4 Personal data shall be accurate and where necessary kept up to date; every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay (*'accuracy'*).

This means the Trust shall take all reasonable efforts to ensure the personal data it holds is accurate and where necessary kept up to date, and where personal data is found to be inaccurate, this information shall be corrected or erased without delay.

The Trust shall send reminders, on at least an annual basis, to parents/carers, pupils and employees, asking them to notify the Trust of any changes to their contact details or other information. The Trust shall also carry out periodic sample checks of pupil and employee files to ensure the data is accurate and up to date.

6.5 Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed (*'storage limitation'*).

This means the Trust shall not keep personal data for any longer than it needs to. Personal data may be stored for longer periods where it is solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, provided that appropriate technical and organisational measures are in place to safeguard the rights and freedoms of the data subject.

The Trust shall maintain and follow a Record Retention Schedule which sets out the timeframes for retaining and disposing of personal data. This schedule shall be published alongside the Trust's privacy notices on the website [here](#).

The Trust shall designate responsibility for record retention and disposal to data leads, who shall adhere to the Trust's Record Retention Schedule and ensure the timely and secure disposal of the data.

6.6 Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. (*'integrity and confidentiality'*)

This means the Trust shall have appropriate security in place to protect personal data. The following are examples of the minimum technical and organisational measures that shall be in place to protect personal data:

6.7 Technical security measures:

- Security patches shall be applied promptly.

- Access to systems shall be restricted according to role-based requirements.
- Strong password policies shall be enforced; passwords shall be a minimum of 8 characters in length; changed at appropriate intervals and not shared or used by others. Password managers shall be utilised where possible.
- Portable devices (such as laptops) and removable media (such as USBs) storing personal data shall be encrypted.
- Data shall be backed up regularly.
- The Trust's disaster recovery and business continuity plans shall be regularly tested to ensure data can be restored in a timely manner in the event of an incident.
- Two factor authentication (2FA) shall be enabled on systems containing sensitive data.

6.8 Organisational security measures:

- Employees shall sign confidentiality clauses as part of their employment contract.
- Mandatory data protection awareness training shall be provided to employees and governors during onboarding and annually thereafter.
- Cyber security training, guidance or advice shall be cascaded to employees on a regular basis.
- Policies and guidance shall be communicated to employees and governors on the secure handling of personal data in Trust and when working remotely.
- Data protection compliance shall be a regular agenda item in governing body and Senior Leadership Team meetings. All employees shall be given the opportunity to raise compliance queries or concerns at any meeting.
- Cross cutting shredders and/or confidential waste containers will be available on the Trust's premises and used to dispose of paperwork containing personal data.
- Appropriate equipment and guidance will be available for employees to use and follow when carrying confidential paperwork off Trust premises.
- The Trust's buildings, offices and where appropriate classrooms, shall be locked when not in use.
- Paper documents and files containing personal data shall be locked in cabinets/cupboards when not in use, and access restricted on a need-to-know basis.
- Procedures shall be in place for visitors coming onto the Trust's premises. These will include signing in and out at reception, wearing a visitor's badge and being escorted where appropriate.
- The Trust shall have procedures in place to identify, report, record, investigate and manage personal data breaches in the event of a security incident.

The Trust shall have appropriate records in place to demonstrate compliance with each of these data protection principles ('accountability').

7 Data subjects' rights

Data subjects have several rights under the data protection legislation. The right to:

- be told how their personal data is being processed.

- request access to their personal data.
- request that inaccurate or incomplete personal data is rectified.
- request the erasure of personal data in certain circumstances.
- request the processing of their personal data is restricted in some circumstances.
- request that their personal data is transferred from one organisation to another or given to them, in certain circumstances.
- object to their personal data being used for public interest or direct marketing purposes.
- prevent important decisions being made about them by solely automated means (including profiling).
- complain to the Trust about the handling of their personal data. If they remain dissatisfied with Trust's response, they have the right to escalate this to the Information Commissioner's Office.

Data subjects may exercise their data protection rights by contacting the Trust in writing or verbally. Data subjects are recommended to submit their request in writing and send this to The Harbour Schools Partnership, Woodwater Academy, Woodwater Lane, Exeter, EX2 5AW or email info@phplaw.co.uk with the subject heading [Data Subject Request – The Harbour Schools Partnership](#). The Trust shall handle all Data Protection Requests in line with the Data Protection Request Handling Procedure.

8 Personal data breaches

The Trust shall follow the Personal Data Breach Handling Procedure in the event of a personal data breach. A personal data breach is a:

'breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed'

Examples of personal data breaches include, but are not limited to:

- Emailing a group of parents and failing to insert their private email addresses into the 'Bcc' field, thus revealing those email addresses to all recipients.
- Emailing or posting confidential information to the wrong person.
- Not storing or disposing of confidential paperwork securely.
- Loss or theft of IT equipment which has personal data stored on it eg a laptop, iPad, mobile phone or a USB.
- Altering, sharing or destroying personal data records without permission from the Trust.
- Using another person's login credentials to gain higher level access to records.
- Sharing login details or having insufficient access controls to systems, which result in unauthorised viewing, use, modification or sharing of personal data.
- Hacking into a system containing personal data.
- A social engineering incident whereby a person uses deception to manipulate individuals into divulging confidential or personal information eg a phishing email.
- A cyber-attack resulting in loss of access to personal data (eg a ransomware attack).
- Environmental incidents such as a fire or flood which damage or destroy important personal data records, prior to their scheduled disposal.
- An employee abusing their access privileges to look at someone else's records out of personal curiosity or gain.

All personal data breaches and suspected breaches (including cyber incidents) shall be reported to the Data Protection Officer immediately [through](#) the GDPR Portal

All incidents shall be recorded within the GDPR Portal and investigated by a member of the Senior Leadership Team (or other person as appropriate), under the support and direction of the Data Protection Officer. Cyber incidents shall be reported to and investigated by the Trust's IT Manager or Security Manager who shall keep the Data Protection Officer informed of their findings where personal data has been compromised.

8.1 Notification to the ICO and Data Subjects

The Data Protection Officer shall determine whether the Trust must notify the Information Commissioner's Office and data subjects following a personal data breach.

A personal data breach is required to be reported to the ICO within 72hrs of the Trust becoming aware of the breach, where the breach is likely to result in a risk to the data subject or someone else, for example if they are likely to suffer damage, discrimination, disadvantage or distress.

Data subjects are required to be informed without undue delay, where the breach is likely to result in 'high risks', for example if the breach could lead to identity theft, psychological distress, humiliation, reputational damage or physical harm.

The Data Protection Officer shall notify the ICO (following consultation with the Trust) where a personal data breach meets the 'risk' threshold. The Headteacher or other delegated employee shall notify data subjects (or their parents) following a 'high risk' breach.

9 Sharing data

The Trust regularly shares personal data internally and externally with partner agencies and third parties for legitimate purposes. Employees shall follow to the Trust's policies and procedures when sharing personal data and adhere to the statutory and non-statutory guidance as set out in the:

- HM Government: Information Sharing Advice for Safeguarding Practitioners (2023)
- Department for Education: Keeping Children Safe in Education (2024)
- Information Commissioner Office: Data Sharing Code of Practice (2020)

When sharing personal data with third parties the Trust shall adhere to the following principles:

- Data subject(s) shall be made aware of the sharing through privacy notices or specific communications regarding the sharing.
- An appropriate lawful basis shall be identified prior to the sharing.
- Data shared shall be adequate, relevant and limited to what is necessary.
- Accuracy of the data shall be checked prior to the sharing (where possible).
- Expectations regarding data retention shall be communicated.
- Data shall be shared by secure means and measures in place to protect the data when received by the third party.
- A record shall be kept of the data sharing.
- Information sharing agreements shall be in place where required.

The Trust understands the data protection laws expressly allow organisations to share necessary and proportionate personal data with third parties to protect the safety or well-being of a child and in urgent or emergency situations to prevent loss of life or serious physical, emotional or mental harm, and is not a barrier to sensible and necessary sharing.

9.1 Sharing data with suppliers (data processors)

The Trust uses a variety of service providers to help it run effectively. These are sometimes referred to as 'data processors'. This often includes companies providing services such as IT support, professional advice (eg human resources, legal advice, insurers and auditors), learning or teaching resources, management information systems, parent communication platforms, document storage solutions, catering and transport.

Using these service providers usually requires disclosing personal data to them so they can deliver the service or product the Trust has purchased. The data protection legislation requires that before sharing personal data with a service provider, the Trust must carry out due diligence checks on the company or product to assess they have appropriate measures in place that ensures compliance with the data protection legislation and protects the rights of data subjects.

Due diligence checks shall be carried out on prospective service suppliers by the Trust, alongside the Data Protection Officer. The outcome shall be recorded on the Trust's Data Processor Due Diligence Report template.

Employees shall not purchase a product or service which involves the disclosure of personal data, unless the appropriate due diligence checks have been carried out in consultation with the Data Protection Officer, and the product has been approved by a member of SLT (or other delegated person).

10 Data Protection Impact Assessments

The Trust is required to carry out Data Protection Impact Assessment (DPIAs) on the processing of personal data, where this is likely to result in 'high risks' to the rights and freedoms of data subjects. High risk means the potential for any significant physical, material or non-material harm (eg distress) to individuals.

A DPIA is a process which helps the Trust identify, minimise and document the data protection risks of a project or plan involving personal data. It demonstrates the Trust's compliance with the data protection principles and fulfils its 'accountability' and 'data protection by design' obligations. A DPIA does not have to eradicate all risk but should minimise risks and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what the Trust wants to achieve.

The UK GDPR sets out three types of processing which will always require a DPIA:

- Systematic and extensive evaluation or profiling of individuals with significant effects
- Large scale use of sensitive data (special category or criminal conviction or offence data)
- Systematic monitoring of a publicly accessible area on a large scale

The Trust shall follow the Information Commissioner's Office supplementary list of processing, which also requires a DPIA:

- Use of innovative technology (such as Artificial Intelligence (AI))
- Denial of a service, opportunity or benefit
- Large scale profiling
- Processing of biometric or genetic data
- Data matching
- Invisible processing
- Tracking
- Targeting children or other vulnerable individuals
- Risk of physical harm

The Trust shall also consider the European guidelines (Guidelines on Data Protection Impact Assessment), to help identify other likely high risk processing, which includes:

- Use of sensitive data or data of a highly personal nature.
- Data concerning vulnerable data subjects.
- Innovative use or applying new technological or organisational solutions.

The Trust shall use their DPIA pre-screening checklist to help identify whether a DPIA should be carried out. The results from DPIAs shall be recorded and shared with the Data Protection Officer, who will advise on any privacy risks and mitigations that can be made to reduce the likelihood of these risks materialising. The Data Protection Officer will monitor the outcome of the DPIA to ensure the mitigations are put in place. DPIAs shall be reviewed on an annual basis.

11 Records management

Records management is a system for managing records throughout their life cycle, from the time of creation or receipt to their destruction. The Trust recognises that good records management plays a crucial role in the smooth running of the Trust and is also necessary to comply with its obligations under the data protection legislation and the Freedom of Information Act 2000, particularly when responding to information access requests and protecting personal data from security threats.

The Trust shall manage its electronic and paper-based records in line with the statutory Code of Practice on the Management of Records, issued under section 46 of the Freedom of Information Act 2000.

Employees and governors shall be provided with advice, guidance and training on how to manage the Trust's records effectively throughout their lifecycle. This should include naming, storing, accessing, security classification, and disposal of records.

The Trust shall maintain a record retention schedule and regularly review its records to ensure they are disposed of in line with the schedule. The schedule shall be communicated to data leads responsible for managing the Trust's records.

11.1 Record of processing activities

The Trust shall, amongst other things, know what personal data records it holds, who it shares these records with; the security in place to protect them and how long they are to be kept for. This information shall be recorded in Data Map, in line with Article 30 of the UK GDPR. The Data Maps will be stored within the GDPR Portal for each school, shall be reviewed annually and made available to the Information Commissioner upon request.

Links to other Trust Policies

List any other policies or guidance that is referenced within this policy document

Freedom of Information Policy

Privacy Notices

Records Management Schedule

Policy history

Policy Version and Date	Summary of Change	Amended by	Implementation Date
Version 1.7 Sept 25	Sections 4.4.2, 4.4.3, 7.2, 8.3, 8.4, 11.5 of policy updated post-merger to reflect change of DPO to John Walker of PHPLaw Ltd and the use of GDPR a portal for breach management and storage of data maps & DPIA's. Section 6 wording unchanged, numbering rationalised to principle headings	Amended by	Implementation Date

Version 1.6	2.2 Insertion of an additional bullet point: <i>'Appropriate Policy Document'</i> 4.5.5 Insertion of new paragraph: re right to monitor employees use of systems 6.25 Insertion of new bullet point: procedures to wipe data from redundant equipment 8.3 Insertion of addition wording: <i>'or directly to dpo@firebirdltd.co.uk'</i> 9.1 DfE and ICO guidance dates updated 9.4.1 Paragraph amended: 9.4.2 Insertion of <i>'or subscribed to.'</i> 9.4.3 Insertion of <i>'prior to using the service or product provided by the supplier'</i> 9.4.4 Insertion of <i>'a data processing agreement is in place'</i> 10.4 Insertion of <i>'including the use of'</i>	Data Protection Officer	Xx xx 2024
Version 1.5	This policy has been re-written to simplify and re-order the existing content and includes new content (Records Management). This policy replaces the Trust's existing Data Protection Policy in its entirety.	Data Protection Officer	Xx xx 2023
Version 1.4	5.2.2 all bullet points re-worded and simplified 5.2.3 all bullet points re-worded and simplified 5.2.6 all bullet points reworded 5.8.1 insertion of new bullet point re 2fa 5.9.1, 5.10.2, 5.14.2 updated re Cyber security & training 5.15, 5.17 minor rewording 5.18 insertion of new section	Data Protection Officer	Xx xx 2022
Version 1.3	1.1. 5.14.3, 5.15.1, 5.18.1 – removal of the reference 'EU GDPR' changing this to <i>'UK GDPR'</i> 2.2 – reference to other relevant policies 4.4.4 –awareness of <i>Data Protection Act 2018 and/or the Computer Misuse Act 1990.</i> 5.1.2 – insertion of new sentence to read: <i>The Trust shall have appropriate measures and records in place to demonstrate compliance with the data protection principles.</i> 5.1.3 – renumbering of existing paragraph 5.2.2 & 5.14.2, 5.15.1, 5.16.2, 5.16.6 minor rewording Removal of employee declaration form		
Version 1.2 July 2020	5.2.3 amended re special categories of personal data 5.2.11 updated re privacy notices removal of 5.2.12, 5.2.13, 5.2.14 5.53, 5.10.1 minor wording amendments		
Version 1.1 July 2019	Section 4 updated to reference Headteacher ort Principal Updated for change of DPO to Amber Bradley of Firebird		

	5.2.7 amended to include: <i>Accessing infor children aged 13 & over</i> 5.2.12, 5.2.13, 5.11.1 amendments relating to privacy notices Renumbering of paragraphs in section 5.11-5.12		
Version 1.0 25 May 2018	This policy replaces the Trust's existing Data Protection Policy	Data Protection Officer	25 May 2018

Appendix 1 Data Protection Policy Definitions

Term Used	Summary Definition
Personal data	Personal data means any information relating to an identified or identifiable living individual. This includes a name, identification number, location data, an online identifier, information relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
Special categories of personal data	Special categories of personal data mean personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs and the trade union membership of the data subject. It also includes the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health, and data relating to an individual's sex life or sexual orientation.
Processing	Processing means any operation or set of operations which is performed on personal data, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data subject	An identifiable, living individual who is the subject of personal data.
Data controller	A data controller is an organisation who determines the purposes and means of the processing of personal data.
Data processor	A data processor is an individual or organisation who processes personal data on behalf of a data controller, upon their instructions.