Data Protection Policy

Policy Code:	HR6
Policy Start Date:	March 2024
Policy Review Date:	March 2027

Please read this policy in conjunction with the policies listed below:

- HR5 Acceptable Use (ICT) Policy
- HR6A Data Breach Policy
- HR12 Staff Disciplinary Policy
- HR33 Records Managements Policy
- HR36 Complaints Policy
- ICT1 CCTV Policy
- ICT2 Online Safety Policy (Staff)
- ICT3 Online Safety Policy (Students)
- SW5 Safeguarding and Child Protection (Promoting Students Welfare) Policy
- SW9 Parental Communication and Complaints Policy
- SW17 Safeguarding Adults

1 Policy Statement

1.1 The policy outlines the Trust's approach to data protection and how it handles personal data.

1.2 This policy applies to all members of staff and agents of The Priory Federation of Academies Trust (the Trust), and to contractors, suppliers and consultants employed by the Trust, insofar as they may collect, hold, access or dispose of personal data relating to the business of the Trust.

1.3 The provisions of this policy extend to personal data held on any personal computers or personal organisers, or in structured manual files, even if not owned by the Trust, when used by members of staff, or external contractors and advisors, specifically to support the business activities of the Trust (e.g., smart phones, tablets, laptops or home PCs by staff for business purposes).

1.4 Compliance with this Policy is mandatory and any breach of the Data Protection Act 2018 will be dealt with in line with the Trust's HR6A Data Breach Policy.

1.5 References to the Trust or Academy within this policy specifically include all nursery, primary, secondary and special academies within the Trust, as well as Priory Apprenticeships and Lincolnshire ITT.

1.6 This policy does not form part of any member of staff's contract of employment and it may be amended at any time.

2 Roles, Responsibilities and Implementation

2.1 The People, Performance and Operations Committee has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. This committee delegates day-to-day responsibility for operating the policy and ensuring its maintenance and review to the Data Protection Officer.

2.2 This policy is approved by the People, Performance and Operations Committee before being ratified at the next available Trust Board meeting. Approval and ratification is minuted, with records kept by the Clerk to Trustees.

2.3 Leaders and Managers have a specific responsibility to ensure the fair application of this policy and all staff are responsible for supporting colleagues and ensuring its success.

2.4 It is the responsibility of all staff to manage their own security by keeping passwords secure and ensuring others do not use their credentials. Any security concerns must be reported to IT support.

2.5 It is the responsibility of all staff to ensure that all records are as accurate and up-to-date as possible, ensuring changes to personal data are promptly reported to the Data Teams to allow the Academies' Management Information System (MIS), to be maintained. Staff can, and have a responsibility to, update their own personal information within the Employee Self-Service (ESS) element of iTrent.

3 Aims

3.1 The Trust aims to ensure that all personal data collected about staff, students, parents/carers, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (UK-GDPR) and the Data Protection Act 2018 (DPA 2018).

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

4 Policy Details

4.1 The Trust aims to ensure that all personal data collected about staff, students, The Trust collects and uses personal information about staff, students, parents/carers and other individuals who come into contact with any of its Academies and Federation Services. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Trust complies with its statutory obligations.

4.2 The Trust has a duty to be registered, as Data Controller, with the Information Commission (ICO) detailing the information held and its use. These details are then available on the ICO's website. The Trust also has a duty to issue a Privacy Notice to all students/parents and staff; this summarises the information held on students/staff/contractors, why it is held and the other parties to whom it may be passed on.

5 Legislation

5.1 This policy meets the requirements of the UK GDPR and the Data Protection Act 2018. It is based on guidance published by the Information Commission on the UK GDPR and the ICO's code of practice for subject access requests.

5.2 It meets the requirements of the Protection of Freedoms Act 2012 when referring to an Academy's use of biometric data.

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

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

6 Terminology

6.1 The Trust processes personal data relating to parents/carers, students, staff, governors, visitors and others, and therefore is a data controller. The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual (Data Subject). This may include the individual's: – Name (including initials) – Identification number – Location data – Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity or an opinion about that person's actions or behaviours.
Special categories of personal data	Personal Data which is more sensitive and so needs more protection, including information about an individual's: – Racial or ethnic origin – Political opinions – Religious or philosophical beliefs – Trade union membership – Genetics – Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes – Health – physical or mental – Sex life or sexual orientation
Processing	Anything done to Personal Data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, transferring, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable, living individual whose Personal Data is held or Processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than a member of staff of the data controller, who processes personal data on behalf of the data controller.
Personal Data Breach	A breach or compromise of security, confidentiality, integrity or availability of Personal Data, leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to such Personal Data.

7 Data Protection Principles

7.1 The UK GDPR is based on data protection principles that The Trust must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.
- Not transferred to another country without appropriate safeguards being in place.
- Made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data.

7.2 The Trust is responsible for and must be able to demonstrate compliance with these principles. This policy sets out how the Trust aims to comply with these principles.

8 Handling data

8.1 **Lawfulness, fairness and transparency -** Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.
We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- the data needs to be processed so that the Trust can fulfil a contract with the Data Subject, or the Data Subject has asked the Trust to take specific steps before entering into a contract;
- the data needs to be processed so that the Trust can comply with a legal obligation;
- the data needs to be processed to ensure the vital interests of the Data Subject e.g. to protect someone's life;
- the data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest, and carry out its official functions;
- the data needs to be processed for the legitimate interests of the Trust or a third party (provided the individual's rights and freedoms are not overridden); and
- the Data Subject (or their parent/carer when appropriate in the case of a student) has freely given clear consent.

8.2 For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

8.3 If any of the Trust's Primary Academies offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent.

8.4 If any of the Trust's Secondary Academies offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is 13 or under.

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

9 Consent

9.1 The Trust will only process Personal Data on the basis of one or more of the lawful bases, including Consent.

9.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are

unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

9.3 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if the Trust intends to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

9.4 When processing Special Category Data or Criminal Convictions Data, the Trust will usually rely on a legal basis for processing other than Consent if possible.

9.5 The Trust will need to evidence Consent and keep records in order to demonstrate compliance with Consent requirements.

10 Transparency

10.1 The legislation requires the Trust to provide detailed, specific information to Data Subjects through appropriate Privacy Notices which the Data Subject can easily understand.

10.2 Data Subjects have the right to know how and why the Trust will use, Process, disclose, protect and retain their Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

11 Limitation, minimisation and accuracy

11.1 The Trust will only collect personal data for specified, explicit and legitimate reasons. These reasons will be shared with the individuals when the data is first collected.

11.2 If personal data is to be used for reasons other than those given when it was first obtained, the individuals concerned will be informed and consent will be sought where necessary.

11.3 Staff must only process personal data that is relevant and limited to what is necessary in order to do their jobs. Personal Data must not be processed for any reason unrelated to the job and should not be excessive.

11.4 When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's HR33 Records Managements Policy.

11.5 The Trust will ensure that Personal Data it holds is accurate, complete, kept up to date and is relevant to the purpose for which it is collected. Data will checked for accuracy at point of collection and at regular intervals afterwards. Reasonable steps will be taken to destroy or amend inaccurate or out of date Personal Data.

12 Sharing personal data

12.1 The Trust will not normally share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The Trust may share the Personal Data where:

- there is an issue with a student or parent/carer that puts the safety of our staff at risk. If outside agencies are liaised with then verbal consent will be sought as necessary; and/or
- suppliers or contractors need data to enable the Trust to provide services to staff and students – for example, IT companies.

12.2 If data is shared with suppliers or contractors then the Trust is committed to:

- only appointing suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
- establishing a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data which is shared; and
- only sharing data that the supplier or contractor needs to carry out their service.

12.3 The Trust will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- the prevention or detection of crime and/or fraud;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax owed to HMRC;
- in connection with legal proceedings;
- where the disclosure is required to satisfy our safeguarding obligations; and/or
- research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

12.4 We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

12.5 The Trust recognises that UK GDPR and the Data Protection Act 2018 are not barriers to safeguarding information sharing. Where safeguarding concerns exist, personal data may be shared where an appropriate lawful basis exists, in line with the statutory DfE guidance 'Information Sharing Duty'.

12.6 The Trust may also share your information with other third parties, if:

- they have a need to know the information for the purposes of providing the contracted services; and/or
- sharing the Personal Data complies with the Privacy Notice and, if required, the Data Subject's consent has been obtained.

13 Subject Access Requests and other rights of individuals

13.1 **Subject Access Requests (SAR) -** Individuals have rights when it comes to how the Trust handles their Personal Data and gain access to personal information that the Trust holds about them. This includes:

- confirmation that their personal data is being processed;
- access to a copy of their Personal Data;
- the purposes of the data processing;
- the categories of personal data concerned;
- who the data has been, or will be, shared with;
- how long the data will be stored for, or if this isn't possible, the criteria used to determine this period;
- the source of the data, if not the individual; and
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

13.2 Subject access requests should be submitted in writing, either by letter or email.

Email: SAR@prioryacademies.co.uk

Letter: Subject Access Request
The Priory Federation of Academies Trust
Trust Offices
Clayton Road
Lincoln
Lincolnshire
LN5 8RE

They should include:

- name of individual;

- correspondence address;
- contact number and email address; and
- details of the information requested

13.3 If staff receive a subject access request, they must immediately forward it to this email address: SAR@prioryacademies.co.uk.

13.4 **Young people and Subject Access Requests (SAR) -** Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

13.5 Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students under 12 within the Trust may be granted without the express permission of the student, whereas for children aged 12 and above most subject access requests from parents or carers of students may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

13.6 Responding to Subject Access Requests - When responding to requests:

- the individual may be asked to provide 2 forms of identification;
- the individual may be contacted via phone if further clarification is needed;
- upon verification and clarification of a request (where applicable), the Trust shall conduct reasonable and proportionate searches in relation to the requested data;
- a response will be made without delay and normally within 1 month of receipt of the request. Where a request is complex or numerous, it may take 3 months from receipt of the request. The individual will be informed of this within 1 month, along with an explanation as to why the extension is necessary; and
- the information will in most cases be provided free of charge.

13.7 The timeframe related to the request shall be paused/delayed in, but not limited to, the following circumstances:

- in order for the Trust to verify the identity of the data subject or their parent/carer;
- when requesting a clarification due to the initial request being unclear;
- when requesting additional information necessary to process the request; or
- when dealing with complex or multiple requests from the same individual.

13.8 Information will not be disclosed if it:

- might cause serious harm to the physical or mental health of the student or another individual;
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- is contained in adoption or parental order records; and/or
- is given to a court in proceedings concerning the child.

13.9 If the request is unfounded or excessive, the Trust may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is for example repetitive, asks for further copies of the same information or fulfilling the request would require unreasonable or disproportionate searches (as determined by the Trust).

13.10 When a request is refused, the individual will be told why and that they have the right to complain to the Trust and, if still unsatisfied, to the ICO.

14 Other data protection rights of the individual

14.1 In addition to the right to make a subject access request, and to receive information when their data is being collected, how it is used and processed, individuals also have the right to:

- withdraw their consent to processing at any time, where consent is the only lawful base on which the processing is carried out;
- ask the Trust to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- prevent use of their personal data for direct marketing;
- challenge processing which has been justified on the basis of public interest;
- request a copy of agreements under which their personal data is transferred outside of the European Economic Area;
- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
- prevent processing that is likely to cause damage or distress;
- be notified of a data breach in certain circumstances;
- make a complaint to the ICO; and
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

14.2 Individuals should submit any request to exercise these rights to the Data Protection Officer (DPO). If staff receive such a request, they must immediately forward it to the DPO. The contact for the DPO is: DPO@prioryacademies.co.uk

15 Biometric recognition systems

15.1 Biometric data means personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements. The Information Commission considers all biometric information to be personal data as defined by the Data Protection Act 2018; this means that it must be obtained, used and stored in accordance with that Act.

15.2 An automated biometric recognition system uses technology which measures an individuals' physical or behavioural characteristics by using equipment that operates 'automatically' (i.e., electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify the individual.

15.3 The Trust will adhere to the DfE document *Protection of biometric information of children in schools and colleges.*

15.4 Where students' biometric data is used as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash), the Trust will comply with the requirements of the Protection of Freedoms Act 2012 and the Data Protection Act 2018.

15.5 Each parent of a student will be notified before any biometric recognition system is put in place or before their child first takes part in it. Where the child is under the age of 18 the Academy will get written consent from at least one parent or carer before any biometric data is taken from their child and it is processed.

15.6 The Trust will not process the biometric data of a student (under the age of 18) where:

- the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;
- no parent or carer has consented in writing to the processing; or
- a parent or carer has objected in writing to such processing, even if another parent or carer has given written consent.

15.7 The Academy will provide reasonable alternative means of accessing services for those students who will not be using an automated biometric recognition system.

15.8 Parents/carers and students can object to participation in the Academy's biometric recognition system(s), or withdraw consent, at any time, and any relevant data already captured will be deleted.

15.9 As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, their data will not be processed irrespective of any consent given by the pupil's parent(s)/carer(s).

16 CCTV

16.1 The Trust uses CCTV for the purposes of student, staff and public safety and crime prevention and detection. The Trust adheres to the ICO's code of practice for the use of CCTV. For further information please see the Trust's ICT1 CCTV Policy.

16.2 An individuals' permission is not needed in order for CCTV to be used, but it is made clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

16.3 Any enquiries about the CCTV system should be directed to DPO@prioryacademies.co.uk.

17 Photographs and videos

17.1 Written consent will be obtained from parents/carers, or students aged 16 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

17.2 Where parental consent is needed, it will be clearly explained how the photograph and/or video will be used. Where parental consent is not needed, we will clearly explain to the student how the photograph and/or video will be used. Uses may include:

- within the academies on notice boards and in Academy (or Trust) magazines, brochures, newsletters, etc;
- outside of the Academy by external agencies such as the academy photographer, newspapers, media campaigns; and/or
- online on the Trust (or individual Academy) website or social media pages.

17.3 Consent can be refused or withdrawn at any time. If consent is withdrawn, the photograph or video will, where possible, be deleted from electronic media or social media accounts held by the Trust and it will not be distributed by the Trust any further.

18 Accountability

18.1 The following technical and organisational measures will be in place to show integrated data protection into all data processing activities, including:

- appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law;
- completing privacy impact assessments where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies;
- integrating data protection into internal documents including this policy, any related policies and privacy notices;
- regularly training members of staff on data protection law, this policy, any related policies and any other data protection matter; and
- regularly conducting reviews and audits to test privacy measures and ensuring compliance.

19 Record Keeping

19.1 The Trust is legally required to keep full and accurate records of all its data Processing activities. Maintaining records of processing activities, including:

- for the benefit of data subjects, making available the name and contact details of the DPO and all information we are required to share about how we use and process their personal data (via our privacy notices);
- for all Personal Data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure; and
- the Trust will keep a record of the Data Subject's consent and procedures for obtaining consent.

20 Data security and storage of records

20.1 The Trust will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or

unlawful loss, destruction or damage. All staff are also responsible for protecting the Personal Data held by the Trust. All staff are required to implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against accidental loss of, or damage to, Personal Data. In particular, staff are required to follow procedures the Trust has in place to maintain the security of all Personal Data.

In particular:

- paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept in a secure location when not in use;
- papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- passwords that are at least 8 characters long containing letters and numbers are used to access academy computers, laptops and other electronic devices;
- students may be asked to change their password if there are concerns about the security of their current one; and
- where personal data needs to be shared with a third party, reasonable steps are taken to ensure it is stored securely and adequately protected and it is only shared on a need to know basis.

20.2 The Trust will evaluate and test the effectiveness of those safeguards to ensure security of its Processing of Personal Data.

21 Transfer Limitation

21.1 The legislation restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK law is not undermined. Personal Data originating in one country is transferred across borders when it is transmitted, sent, viewed or accessed in or to a different country.

21.2 Personal Data may also be transferred outside the UK if one of the following conditions applies:

- the UK has issued regulations confirming that the country to which the Trust transfers the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;
- appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved for use in the UK, an approved code

of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

- the Data Subject has provided Consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between the Trust and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

22 Disposal of records

22.1 The Trust will take all reasonable steps to destroy or erase from its system all Personal Data that it no longer requires in accordance with its policies (unless the law requires that data to be kept for a minimum time). For guidance on disposal of records please see HR33 Records Management Policy.

23 Data breaches

23.1 The Trust has put in place procedures to deal with any suspected Personal Data Breaches and will notify Data Subjects or any applicable regulator where it is legally required to do so.

23.2 For guidance on data breaches please see HR6A Data Breach Policy.

24 Training

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

24.2 The Trust is committed to ensuring that data protection training is delivered regularly to all staff and governors.

25 Complaints

25.1 Complaints in relation to the Trust's handling of a Subject Access Request, a Data Breach or any overarching duty in relation to the processing of personal data can be submitted in writing or by email to the details provided below;

Email - DPO@prioryacademies.co.uk

Post – FAO Data Protection Officer, The Priory Federation of Academies, Clayton Road, Lincoln, LN5 8RE.

Any complaint should, as a minimum, include the Data Subject's name, a clear description of the concern and any supporting documentation where relevant.

25.2 Upon receipt of a complaint the Trust shall take the following actions;

- acknowledge receipt within 30 x working days;
- investigate the complaint thoroughly and impartially;
- respond to the complainant with the outcome of the investigation without undue delay; and
- inform the complainant of their right to escalate the matter to the Information Commission in the event that they are dissatisfied with the Trust's response.

25.3 Upon completion of the investigation, any of the below outcomes or findings may be reached:

- the complaint requires no further action;
- there is insufficient evidence to either uphold or dismiss the complaint;
- an acknowledgement that the academy or Trust could have handled the situation differently or better;
- an apology;
- an explanation of steps which have been taken to ensure the circumstances which led to the complaint will not happen again; and/or
- an agreement to review the Trust's policies in light of the complaint.

26 Policy change

26.1 This policy may only be amended or withdrawn by the Priory Federation of Academies Trust.