Data Protection Policy

Policy Code:	HR6
Policy Start Date:	May 2018
Policy Review Date:	May 2021

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 E-Safety Policy
- SW5 Safeguarding and Child Protection (Promoting Students Welfare) Policy

1 Policy Statement

1.1 The policy outlines the Trust's approach to data protection.

1.2 This policy applies to all employees 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 Any breach of the Data Protection Act (2018) will be dealt with in line with the Trust's HR6A Data Breach Policy.

1.5 Wherever referred to, Academy or Trust throughout this policy includes The Robert De Cheney Boarding House at The Priory Academy LSST, the Keyworth Centre at The Priory City of Lincoln Academy, the Early Years Setting at The Priory Witham Academy, Priory Training and the French Centre.

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

2 Roles, Responsibilities and Implementation

2.1 The Pay, Performance and HR 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 Head of Human Resources.

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

2.3 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.

2.4 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 at all times.

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 (GDPR) and the Data Protection Act 2018 (DPA 2018).

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 Commissioner's Office (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 employees; this summarises the information held on students/employees/contractors, why it is held and the other parties to whom it may be passed on.

4.2 Legislation

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

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

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.

4.3 **Terminology**

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

4.4 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.

5 Data Protection Principles

The 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

This policy sets out how the Trust aims to comply with these principles.

6 Handling data

6.1 Lawfulness, fairness and transparency

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

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual 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 individual 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)
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

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

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.

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.

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

6.2 **Limitation, minimisation and accuracy**

- 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.

- 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.

- Staff must only process personal data where it is necessary in order to do their jobs.

- 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.

6.3 Sharing personal data

The Trust will not normally share personal data with anyone else, but may do so 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.
- Suppliers or contractors need data to enable the Trust to provide services to staff and students – for example, IT companies.

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
- Only sharing data that the supplier or contractor needs to carry out their service

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
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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.

7 Subject Access Requests and other rights of individuals

7.1 Subject Access Requests (SAR)

Individuals have a right to make a ‘subject access request’ to 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 the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with

- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

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

Email:
SAR@prioryacademies.co.uk

Letter:
Subject Access Request
The Priory Federation of Academies Trust
Priory House
Cross O'Cliff Hill
Lincoln
Lincolnshire
LN5 8PW

They should include:

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

If staff receive a subject access request they must immediately forward it to this email address.

7.2 **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.

- 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.

7.3 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 to confirm the request was made
- A response will be made without delay and within 1 month of receipt of the request
- The information will be provided free of charge
- 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

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
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we 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 repetitive, or asks for further copies of the same information.

When we refuse a request, the individual will be told why and that they have the right to complain to the ICO.

7.4 Other data protection rights of the individual

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
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the 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**

8 Biometric recognition systems

- Where student' 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.

- Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. 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.

- Parents/carers and students have the right to choose not to use the Academy's biometric system(s). Alternative means of accessing the relevant services for those students will be provided. For example, student can pay for school dinners in cash at each transaction if they wish.

- 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.

- 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).

9 CCTV

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.

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.

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

10 Photographs and videos

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.

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
- Online on the Trust (or individual Academy) website or social media pages

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

11 Data protection by design and default

The following 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 matters

- Regularly conducting reviews and audits to test privacy measures and ensuring compliance

- 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

12 Data security and storage of records

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.

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. Staff must change their passwords at least once a year

and students are reminded to change their passwords at regular intervals. Students may be asked to change their password if there are concerns about the security of their current one

- Where personal data needs to be shared with a third party, reasonable steps are taken to ensure it is stored securely and adequately protected

13 Disposal of records

For guidance on disposal of records please see HR33 Records Management Policy.

14 Data breaches

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

15 Training

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

The Trust is committed to ensuring that data protection training is delivered regularly (at least annually) to all staff and governors.

16 Complaints

Complaints will be dealt with in accordance with the Trust's HR36 Complaints Policy. Complaints relating to information handling may be referred to the Information Commissioner's Office (ICO).

17 Policy change

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

The Priory Federation of Academies Trust

Data Protection Policy

This Policy has been approved by the Pay, Performance and HR Committee:

Signed…… Name..... Date:

Trustee

Signed…… Name..... Date:

Chief Executive Officer

Signed…… Name..... Date:

Designated Member of Staff

Please note that a signed copy of this agreement is available via Human Resources.