Records Management Policy

Policy Code:	HR33
Policy Start Date:	March 2020
Policy Review Date:	March 2021

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

- HR6 Data Protection Policy
- HR6A Data Breach Policy
- HR12 Staff Disciplinary Policy
- HR33 Records Managements Policy
- HR36 Complaints Policy
- ICT2 E-Safety Policy
- SW5 Safeguarding and Child Protection (Promoting Students Welfare) Policy

1 Policy Statement

1.1 As a public body, the Trust is required by law to manage records appropriately. Legislation such as the Data Protection Act 2018, Freedom of Information Act 2000 and Environmental Information Regulations 2004 set out specific requirements in relation to the creation and management of records.

1.2 Maintaining appropriate and effective records management practices will help the Trust to deliver and meet our statutory duties. By adopting this policy the Trust aims to ensure that the record, in whatever form it takes, is accurate, reliable, ordered, complete, useful, up to date and accessible whenever it is needed.

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

1.4 References to the Trust or Academy within this policy specifically include all primary, secondary and special academies within the Trust, as well as Robert De Cheney Boarding House, the Early Years setting at the Priory Witham Academy, Priory Training, Priory Apprenticeships, Lincolnshire Teaching School Alliance and Lincolnshire Teaching School Alliance SCITT.

1.5 The Trust is committed to leading a mentally healthy organisation, which includes a commitment to and promotion of emotional wellbeing and mental health. Therefore, all Trust policies and procedures ensure this commitment is incorporated in order to support all staff and students. Members of staff are encouraged to speak to their line managers, and students are encouraged to speak to any member of staff, if they feel any part of this policy would affect their emotional wellbeing and mental health. Any such comments should be passed to the Trust's HR department (via FederationHR@prioryacademies.co.uk) for appropriate consideration at the next available point in the policy review cycle.

2 Roles, Responsibility 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 HR Director.

2.2 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.

3 Aims

3.1 To ensure that the Trust manages a record through its life cycle from creation or receipt, through maintenance and use to final disposal (for destruction, transfer or permanent retention).

3.2 To ensure that all Trust staff, governors, trustees, elected members, partners, suppliers and stakeholders are aware of what they must do to manage records in an effective and efficient way.

3.2 To ensure that records are:

- easily and efficiently located, accessed and retrieved;
- better protected and securely stored;
- disposed of safely and at the right time;

3.4 To reduce corporate risk through compliance with relevant legislation.

4 Scope

4.1 This policy shall apply to the management of records in all technical or physical formats or media, created or received by the Trust in the conduct of its business activities.

4.2 This policy applies to all Trust staff (both permanent and temporary), contractors, consultants, volunteers, secondees, elected members, governors, trustees, partners, suppliers and stakeholders who have access to records, wherever these records may be located.

5 Definitions

5.1 **Record:** A record is recorded information, in any form, including data in systems, produced or received and then kept in order to support and/or give evidence of an activity. Since a record is recorded information, no record may be modified.

5.2 **Format:** A record can be in any format including (but not limited to): paper filed, email, audio/visual, electronic documents, systems data, databases, digital images and photographs.

5.3 **Records Management:** The control of records during their lifetime, from creation to storage and retention until the eventual archival preservation or destruction.

5.4 **Records Creator:** The person that produces and receives and then keeps them in its record-keeping system.

5.5 **Record-Keeping System:** System or procedures by which the records are created, captured, secured, maintained and disposed.

5.6 **Records Declaration:** The process through which records are identified as such and distinguished by other information that is not to be regarded as recorded information.

5.7 **Official Copy:** The official copy of a record is the copy intended to give evidence of the activity supported by the record and therefore, if need be, is the one to be submitted to public authorities and other stakeholders and partners.

5.8 **Convenience Copy:** A convenience copy of a record is a copy of a record created for the convenience of the records creator or of someone working for the records creator e.g. to give him/her quicker access to the information contained in the record.

5.9 **Primary Responsibility:** The primary responsibility over a record identifies which organisational unit/person is in charge of keeping the official copy of a record and deciding about specific issues concerning its management.

5.10 **Vital Records:** Records without which an organisation would be unable to function, or to prove that a key activity has taken place.

5.11 **EDRMS:** The Trust's Electronic Documents and Record Management System. The EDRMS may be made up of one or more IT platforms.

6 Official Copies of Records

6.1 There shall be only one official copy of each corporate record.

6.2 If there are two records identical to each other to be kept by the Trust in order to give evidence of two different corporate processes, they shall be considered as two separate records, each one associated with its specific features i.e. retention and disposal schedule, file plan code etc. For example, a member of staff performance report kept both in the personal staff member file of the member of staff and in a litigation file involving the same member of staff.

7 Modifying Records

7.1 Records shall not be modified.

7.2 A new record shall be produced if the information contained in a record is to be corrected, amended or added.

7.3 This former record is to be kept in compliance with the relevant retention and disposal schedule.

8 Access to Records

8.1 Records shall only be accessed by staff for a business purpose.

8.2 Records shall only be disseminated to members of the public in line with the relevant legislation framework and with any other relevant Trust policy and procedure.

8.3 Access to the Trust records which contain personal data shall be granted (exemptions apply) in accordance with The Trust's Subject Access Request procedure (see section 15).

9 Storing Records

9.1 Records shall be kept in a condition so as to ensure continuing authenticity, accessibility, retrievability, intelligibility and usability throughout their whole life-cycle (including, for those selected for long-term or permanent retention, the period when they are kept in the archives).

10 Retention and Disposal

10.1 For retention and disposal schedules the Trust adheres to the Information Management Toolkit for Academies. The only exception to this is the retention and disposal guidelines for Early Years Provision which is included within Appendix 1 of this policy.

10.2 The Trust's retention and disposal schedules shall comply with all relevant UK statutory (including all HMRC) provisions currently in force.

10.3 A Head of Service, who has primary responsibility over the record, shall be required to authorise a change to the retention or disposal schedule following the expiration of a record. If it is in contrast with the original schedule, the reason for the change needs to be documented.

10.4 Legal provisions shall take precedent over proposed modifications.

10.5 The Trust shall ensure that retention and disposal schedules are available to all staff and those managing access to the Trust records.

11 Destruction of Records

11.1 If provided by the relevant retention and disposal schedules, corporate records are to be destroyed when their retention periods expire.

11.2 Before destroying any record, it is necessary to verify that there are no specific circumstances that may prevent the destruction, such as legal holds (issued by a Court) or new business needs e.g. the record might be useful to support either legal defence or another corporate activity.

11.3 Destruction of corporate records shall be authorised in writing by the relevant manager, or authorised deputy, of the service area which has primary responsibility over them.

11.4 The service area which has primary responsibility over the records shall ensure all existing copies of the records are destroyed, regardless of format and location.

11.5 Destruction of records shall be recorded on a Disposal Register (a template is available from HR). The register is to be kept in digital format by the service and a copy sent to the Human Resources Department.

11.6 Paper records are to be destroyed by using the corporately provided lockable confidential disposal bins or confidential waste bags or by shredding the record using a cross cut shredder.

11.7 Confidential waste bags and lockable bins must be kept in a location not accessible to the public. Confidential waste bags are to be held and secured at all times to prevent unauthorised access.

11.8 Microforms, microfiches, microfilms and non-digital photos must be kept separate from paper records and placed in confidential waste bags reserved just for them.

11.9 Electronic records kept in a corporate application shall be deleted using the functionality within the application.

11.10 Sanitisation procedures for ICT storage media holding electronic records which includes optical, magnetic and solid state storage media vary with the media type, but typical methods include overwriting, degaussing and physical destruction. Advice shall be sought from the Information Governance Team when considering the destruction of such media.

11.11 In all instances where ICT storage media is destroyed, a certificate of destruction shall be provided and held as a permanent record by the relevant service area.

12 Convenience Copies of Records

12.1 Corporate retention and disposal schedules do not apply to convenience copies, which are to be destroyed as soon as they are no longer needed to facilitate the work of the person who has produced them.

13 Corporate Record-Keeping System (RKS)

13.1 There shall be an adequate and appropriate allocation of resources by The Trust to maintain its corporate records.

13.2 The Trust shall ensure that corporate records are arranged and identified through the use of a corporate file plan, which also associates them with the relevant retention and disposal schedules.

13.3 The Trust shall ensure records kept are protected from damaging elements such as water, light, temperature, fire, humidity, infestation, digital viruses, power failures, information leakages and security breaches.

13.4 Any Trust off-site storage system shall be considered to be part of the global RKS. Records kept in off-site storage systems shall be managed in compliance with the provisions of this policy.

13.5 The inclusion of a document or a dataset inside the RKS shall amount to declaring it as a record.

13.6 The RKS shall identify and properly keep the official copy of any record.

13.7 Convenience copies of a record are not part of RKS, but shall be managed in compliance with relevant legislation e.g. Data Protection Act 1998 (replaced by GDPR in May 2018), Freedom of Information Act 2000, and provisions concerning legal holds.

13.8 The Trust's Electronic Documents and Record Management System (EDRMS) shall be the primary resource of The Trust's RKS.

13.9 It shall be used to store, manage and keep The Trust's digital records. If the EDRMS consists of more than one IT platform relationships between groups of records shall be highlighted and described through appropriate elements of information.

13.10 It shall be used as the reference point for The Trust's corporate analogue records by indicating in the EDRMS any other record or aggregation of records existing in analogue format. Document Reference: V2.4 Records Management Policy Page 9.

13.11 It shall be used as a reference point for any other digital record not kept in the EDRMS by indicating in the EDRMS any other digital record or aggregation of record existing outside the EDRMS.

13.12 It shall be used as a reference point for corporate records kept in off-site storage systems (including archives records), in the same way as specified at point 13.8 and 13.9.

14 Data Protection

14.1 The Trust shall ensure all records which contain personal data are processed in accordance with the Data Protection Act 2018. Please refer to HR6 Data Protection Policy.

15 Subject Access Requests (SARs)

15.1 The Trust shall ensure that it complies with its obligations under the Data Protection Act 2018 in regards to any SARs.

15.2 For further information or to submit an SAR, please email SAR@prioryacademies.co.uk. For further details of the process please refer to HR6 Data Protection Policy.

16 Information Security

16.1 The Trust shall ensure appropriate security controls are applied to all records.

16.2 The Trust shall ensure that HR5 ICT Acceptable Use Policy is available to all staff.

17 Policy Changes

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

The Priory Federation of Academies Trust
Records Management Policy

This Policy has been approved by the Priory Federation of Academies Trust's 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.

Appendix 1 – Retention Periods

Please note, all files relate to any documents/records saved electronically and in paper format. At present, child protection records must not be destroyed. The retention of such records will be subject to any future instruction given by the national Independent Inquiry into Child Sexual Abuse (IICSA).

1. Early Years Provision

1.1					
	Basic File Description	**Data protection Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
1.1.1	The name, home address and date of birth of each child who is looked after on the premises	Yes		Closure of setting + 50 years (these could be required to show whether or not an individual child attended the setting in a child protection investigation)	Secure Disposal
1.1.2	The name, home address and telephone number of a parent of each child who is looked after on the premises	Yes		If this information is kept in the same book or on the same form as in 9.1.1 then the same retention period should be used as 9.1.1. If the information is stored separately, then destroy once the child has left the setting (unless the information is collected for anything other than emergency contact)	Secure Disposal
1.1.3	The name, address and telephone number of any person who will be looking after children on the premises	Yes		See 2.2.1	Secure Disposal
1.1.4	A daily record of the names of children looked after on the premises, their hours of attendance and the names of the persons who looked after them	Yes	The Day Care and Child Minding (National Standards) (England) Regulations 2003	The regulations say that these records should be kept for 2 years. If these records are likely to be needed in a child protection setting (see 9.1.1) then	Secure Disposal

				the records should be retained for closure of the setting + 50 years	
1.1.5	A record of accidents occurring on the premises and the incident books relating to other incidents	Yes	The Day Care and Child Minding (National Standards) (England) Regulations 2003	DOB of the child involved in the accident or the incident + 25 years. If an adult is injured then the accident book must be kept for 7 years from the date of the incident	Secure Disposal
1.1.6	A record of any medicinal product administered to any child on the premises, including the date and circumstances of its administration, by whom it was administered, including medicinal products which the child is permitted to administer to himself, together with a record of parent's consent	Yes	The Day Care and Child Minding (National Standards) (England) Regulations 2003	DOB of the child being given/taking the medicine + 25 years	Secure Disposal
1.1.7	Record of transfer	Yes		One copy is to be given to the parents, one copy transferred to the Primary School where the child is going	Secure Disposal
1.1.8	Portfolio of work, observations and so on	Yes		To be sent home with the child	Secure Disposal
1.1.9	Birth certificates	Yes		Once the setting has had sight of the birth certificate and recorded the necessary information the original can be returned to the parents. There is no requirement to keep a copy of the birth certificate	Secure Disposal

1.2					
	Basic File Description	**Data protection Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
1.2.1	The name and address and telephone number of the registered person and every other person living or employed on the premises	Yes		See 2.2	Secure Disposal
1.2.2	A statement of the procedure to be followed in the event of a fire or accident	No		Procedure superseded + 7 years	Secure Disposal
1.2.3	A statement of the procedure to be followed in the event of a child being lost or not collected	No		Procedure superseded + 7 years	Secure disposal
1.2.4	A statement of the procedure to be followed where a parent has a complaint about the service being provided by the registered person	No		Until superseded	Secure disposal
1.2.5	A statement of the arrangements in place for the protection of children, including arrangements to safeguard the children from abuse or neglect and procedures to be followed in the event of allegations of abuse or neglect	No		Closure of settings + 50 years (these could be required to show whether or not an individual child attended the setting in a child protection investigation)	Secure disposal

1.3					
	Basic File Description	**Data protection Issues**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
1.3.1	Emergency contact details for appropriate adult to collect the child if necessary	Yes		Destroy once the child has left the setting (unless the information is collected for anything other than emergency contract)	Secure Disposal
1.3.2	Contract, signed by the parent, stating all the relevant details regarding the child and their care, including the name of the emergency contact and confirmation of their agreement to collect the child during the night.	Yes		Date of birth of the child who is the subject of the contract + 25 years	Secure Disposal

1. In this context secure disposal should be taken to mean disposal using confidential waste bins, or if the Academy has the facility, shredding using cross cut shredder.