Pathfinder

Teaching School Alliance

GDPR - Compliant Records Management Policy

This policy explains how records are stored, accessed, monitored, retained and disposed of, in order to meet the alliance's statutory requirements. It ensures we are compliant with the GDPR and should be viewed with the Privacy Policy.

Approval Date: April 2018

Next Review Date: April 2019

Member of staff responsible: Cp – Head of Teaching School

Governance: Teaching School Strategic Board

The Pathfinder Teaching School Alliance School is committed to developing to the full, the potential of each member of the school community, within the context set by its mission and its strategic aims, as teaching schools alliance

Contents

Mission Statement of Pathfinder Teaching School Alliance

The Pathfinder Teaching School Alliance aims to provide the very best education for pupils in our schools. To maximise achievement through collaborative partnerships, a shared vision and by caring for children as individuals.

Aims will be achieved by working within all key areas of "the big three" framework set out in the DfE guidance for teaching schools.

- ***Initial Teacher Training*** – Lead role in recruiting and training teachers of the future
- ***Continuous Professional Development*** – Peer to peer professional and leadership development
- ***School to School Support*** – Providing and coordinating support for other schools

Mission Statement

- To work collaboratively in partnership, as a community of schools, to ensure all children are known and cared for as individuals
- To demonstrate a commitment to every child, to provide the very best education and to maximise achievement
- To share best practice and to provide an environment in which educational theory and practice can be observed, studied and practiced
- To recruit and inspire a new generation of colleagues and existing teachers by establishing the very best professional development to support fellow professionals in raising standards and aspirations
- To work collaboratively with other schools, the Church of England and educational institutions to establish an educational dialogue, to identify and implement change to continually improve practice at all schools
- To develop through partnership and shared values a vision for education

"Values, Care and Achievement lived into being to establish educational excellence through collaborative partnerships"

Our core focus will initially be centred on Initial Teacher Training and Continuous Professional Development. Whilst we will work within the framework of all elements of the "big three" our main priority will be these two components. As capacity and turnover increases, we will gradually expand to develop other areas in more significant detail.

Statement of intent

The Pathfinder Teaching School Alliance is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible by the appropriate individuals. In line with the requirements of the General Data Protection Regulation (GDPR), the alliance also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

The alliance has created this policy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the school's statutory requirements.

This document complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

1. Legal framework

1.1. This policy has due regard to legislation including, but not limited to, the following:
- General Data Protection Regulation (2016)
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)

1.2. This policy also has due regard to the following guidance:
- Information Records Management Society 'Information Management Toolkit for Schools' 2016

1.3. This policy will be implemented in accordance with the following school policies and procedures:
- GDPR policy
- GDPR record management policy
- Data security breach and management policy
- Photograph and Videos policy
- Privacy policy for staff
- Privacy policy for students

2. Responsibilities

2.1. The alliance as a whole has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

2.2. The headteacher holds overall responsibility for this policy and for ensuring it is implemented correctly.

2.3. The data protection officer (DPO) is responsible for the management of records at the teaching school

2.4. The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with the headteacher.

2.5. The DPO is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of correctly.

2.6. All staff members are responsible for ensuring that any records for which they are responsible for are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

3. Management of Trainee Teacher Records

3.1. Trainee Teacher records are specific documents that are prior to, during and after a trainee decides to apply and train with the alliance –

3.2. The following information is stored in a trainee record, and will be easily accessible:

- UCAS Application Form
- Attendance Information
- Trainee Progress Reports/Reviews/Grading
- Notes relating to major incidents
- Information about any additional support trainees may receive (access funds/scholarships)
- DBS details including any criminal disclosures
- Correspondences with partnership schools, the alliance or HEIs
- Notes of complaints
- Interview Records which include: Interview Panel Comments, Pupil Panel Comments, Written Tasks and Reflection Sheets

3.3. The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file that is kept by the Teaching School Administrator:

- Sick notes
- Correspondence with trainees, schools and HEIs about minor issues, e.g. C4C or trainee illness

3.4. Hard copies of disclosures relating to criminal records or serious incidents are retained by the Head of Teaching School and stored in the Head of Teaching Schools office.

3.12. If a trainee enrols on the course, the alliance will keep the trainee's records for six years.

4. Retention of trainee records and other trainee-related information

4.1. The table below outlines the alliance's retention periods for individual trainee records and the action that will be taken after the retention period, in line with any requirements.

4.2. Electronic copies of any information and files will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Admissions		
UCAS application form	Six years after the date on which the student leaves	Information is reviewed and the register may be kept permanently
Interview Documentation	Six years after the date on which the student leaves	Securely disposed of
DBS Information	Until the appeals process has been completed	Securely disposed of
Pupils' educational records		
Trainee Progress Data	Six years after the date on which the student leaves	Securely disposed of
Schools Placement Lists	Six years after the date on which the student leaves	Securely disposed of
Trainee Review Documents	Six years after the date on which the student leaves	Securely disposed of
Cause for Concern Documents	Six years after the date on which the student leaves	Securely disposed of
Supplementary Information on Trainees	Six years after the date on which the student leaves	Securely disposed of
Attendance		
Attendance registers	Six years after the date on which the student leaves	Securely disposed of
Sick Notes/Leave of Absence Documents	Six years after the date on which the student leaves	Securely disposed of
SEND		
Disability Documents	Six years after the date on which the student leaves	Securely disposed of, unless it is subject to a legal hold

5. Retention of staff records

5.1. The table below outlines the teaching school's retention period for staff records and the action that will be taken after the retention period, in line with any requirements.

5.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Operational		
Staff members' personal file	Termination of employment, plus six years	Securely disposed of
Timesheets	Current academic year, plus six years	Securely disposed of
Annual appraisal and assessment records	Current academic year, plus five years	Securely disposed of
Recruitment		
Records relating to the appointment of a new headteacher	Date of appointment, plus six years	Securely disposed of
Records relating to the appointment of new members of staff (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Securely disposed of
Records relating to the appointment of new members of staff (successful candidates)	Relevant information added to the member of staff's personal file.	Securely disposed of
DBS certificates	Up to six months	Securely disposed of
Proof of identify as part of the enhanced DBS check	After identity has been proven	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a copy this will be placed on the staff member's personal file, if not, securely disposed of
Evidence of right to work in the UK	Added to staff personal file or, if kept separately, termination of employment, plus no longer than two years	Securely disposed of
Disciplinary and grievance procedures		
Child protection allegations, including where the allegation is unproven	Added to staff personal file, and until the individual's normal retirement age, or 10 years from the date of the	Reviewed and securely disposed of – shredded

	allegation – whichever is longer If allegations are malicious, they are removed from personal files	
Oral warnings	Date of warning, plus six months	Securely disposed of – if placed on staff personal file, removed from file
Written warning – level 1	Date of warning, plus six months	Securely disposed of – if placed on staff personal file, removed from file
Written warning – level 2	Date of warning, plus 12 months	Securely disposed of – if placed on staff personal file, removed from file
Final warning	Date of warning, plus 18 months	Securely disposed of – if placed on staff personal file, removed from file
Records relating to unproven incidents	Conclusion of the case, unless the incident is child protection related and is disposed of as above	Securely disposed of

6. Retention of Teaching School Strategic Board Records

6.1. The table below outlines the teaching school's retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any requirements.

Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Governing board		
Agendas for strategic board meetings	One copy alongside the original set of minutes – all others disposed of without retention	Securely disposed of
Original, signed copies of the minutes of strategic board meetings	Permanent	
Reports presented to the strategic board	Minimum of six years, unless they refer to individual reports – these are kept permanently	Securely disposed of or, if they refer to individual reports,

		retained with the signed, original copy of minutes
Instruments of government, including articles of association	Permanent	If unable to store, these will be provided to the county archives service
Action plans created and administered by the strategic board	Duration of the action plan, plus three years	Securely disposed of
Policy documents created and administered by the strategic board	Duration of the policy, plus three years	Securely disposed of
Records relating to complaints dealt with by the strategic board	Date of the resolution of the complaint, plus a minimum of six years	Reviewed for further retention in case of contentious disputes, then securely disposed of
Proposals concerning changing the teaching school status	Date proposal accepted or declined, plus three years	Securely disposed of
Teaching School Minutes and Documentation		
Minutes of TS meetings and the meetings of other internal administrative bodies	Date of the meeting, plus three years	Reviewed and securely disposed of
Reports created by the TS	Date of the report, plus a minimum of three years	Reviewed and securely disposed of
Records created by the head of TS, deputy Head of TS or TS administrative team	Current academic year, plus six years	Reviewed and securely disposed of
Correspondence created by the head of TS, deputy Head of TS or TS administrative team	Date of correspondence, plus three years	Reviewed and securely disposed of
Teaching School development plan	Duration of the plan, plus three years	Securely disposed of

7. Retention of health and safety records

7.1. The table below outlines the teaching school's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any requirements.

7.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Health and safety		
Health and safety risk assessments	Duration of risk assessment, plus three years	Securely disposed of
Records relating to accidents and injuries at work	Date of incident, plus 12 years. In the case of serious accidents, a retention period of 15 years is applied	Securely disposed of
Accident reporting – adults	Date of the incident, plus six years	Securely disposed of
Accident reporting – pupils	25 years after the pupil's date of birth, on the pupil's record	Securely disposed of
Control of substances hazardous to health	Current academic year, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with asbestos	Date of last action, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with radiation	Date of last action, plus 50 years	Securely disposed of
Fire precautions log books	Current academic year, plus six years	Securely disposed of

8. Retention of financial records

8.1. The table below outlines the teaching school's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements.

8.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Payroll pensions		

Maternity pay records	Current academic year, plus six years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current academic year, plus six years	Securely disposed of
Risk management and insurance	Current academic year, plus six years	
Employer's liability insurance certificate		Securely disposed of
Asset management		
Burglary, theft and vandalism report forms	Current academic year, plus six years	Securely disposed of
Accounts and statements including budget management		
Annual accounts	Current academic year, plus six years	Disposed of against common standards
Loans and grants managed by the teaching school	Current academic year, plus six years	Information is reviewed then securely disposed of
All records relating to the creation and management of budgets	Current academic year, plus six years	Securely disposed of
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus six years	Securely disposed of
Records relating to the collection and banking of monies	Current financial year, plus six years	Securely disposed of
Records relating to the identification and collection of debt	Current financial year, plus six years	Securely disposed of
Contract management		
All records relating to the management of contracts under seal	Current academic year, plus six years	Securely disposed of
All records relating to the management of contracts under signature	Current academic year, plus six years	Securely disposed of
All records relating to the monitoring of contracts	Current academic year, plus six years	Securely disposed of
School fund		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus six years	Securely disposed of

9. Retention of other teaching school records

9.1. The table below outlines the school's retention periods for any other records held by the school, and the action that will be taken after the retention period, in line with any requirements.

9.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Property management		
Title deeds of properties belonging to the school	Permanent	Transferred to new owners if the building is leased or sold
Plans of property belonging to the school	For as long as the building belongs to the school	Transferred to new owners if the building is leased or sold
Leases of property leased by or to the school	Expiry of lease, plus six years	Securely disposed of
Records relating to the letting of school premises	Current financial year, plus six years	Securely disposed of
Maintenance		
All records relating to the maintenance of the school carried out by contractors	Current academic year, plus six years	Securely disposed of
All records relating to the maintenance of the school carried out by school employees	Current academic year, plus six years	Securely disposed of
Operational administration		
Records relating to the creation and publication of the school brochure and/or prospectus	Current academic year, plus three years	Disposed of against common standards
Records relating to the creation and distribution of circulars to staff, parents or pupils	Current academic year, plus three years	Disposed of against common standards
Newsletters and other items with short operational use	Current academic year plus one year	Disposed of against common standards
Visitors' books and signing-in sheets	Current academic year	Reviewed then securely disposed of
Records relating to the creation and management of parent-teacher associations and/or old pupil associations	Current academic year, plus six years	Reviewed then securely disposed of

10. Storing and protecting information

10.1. The DPO will undertake a risk analysis to identify which records are vital to school management and these records will be stored in the most secure manner.

10.2. Back ups are completed nightly and kept in a different building.

10.3. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.

10.4. Confidential paper records are not left unattended or in clear view when held in a location with general access.

10.5. Staff are not permitted to use storage devices e.g. USB sticks to hold student data.

10.6. All electronic devices are password-protected to protect the information on the device in case of theft.

10.7. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

10.8. All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

10.9. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Names will not be used but initials.

10.10. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

10.11. When sending confidential information by fax, members of staff always check that the recipient is correct before sending.

10.12. Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the GDPR, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

10.13. Before sharing data, staff always ensure that:

- They have consent from data subjects to share it.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.

10.14. All staff members will implement a ‘clear desk policy’ to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.

10.15. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

10.16. The physical security of the school's buildings and storage systems, and access to them, is reviewed termly by the site manager in conjunction with the DPO. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the headteacher and extra measures to secure data storage will be put in place.

10.17. The school takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

10.18. The DPO is responsible for continuity and recovery measures are in place to ensure the security of protected data.

10.19. Any damage to or theft of data will be managed in accordance with the school's Security Breach Management Plan.

11. Accessing information

11.1. The Pathfinder Teaching School Alliance is transparent with data subjects, the information we hold and how it can be accessed.

11.2. All members of staff, parents of registered pupils and other users of the school, e.g. visitors and third-party clubs, are entitled to:

- Know what information the school holds and processes about them or their child and why.
- Understand how to gain access to it.
- Understand how to provide and withdraw consent to information being held.
- Understand what the school is doing to comply with its obligations under the GDPR.

11.3. All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.

11.4. Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents.

11.5. Pupils who are considered to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

11.6. The school will adhere to the provisions outlined in the school's GDPR Data Protection Policy when responding to requests seeking access to personal information.

12. Digital continuity statement

12.1. The data will be archived to dedicated files on the school's server, which are password-protected – this will be backed-up in accordance with section 10 of this policy.

12.2. Memory sticks will never be used to store digital data, subject to a digital continuity statement.

12.3. The IT technician will review new and existing storage methods annually and, where appropriate add them to the digital continuity statement.

12.4. The following information will be included within the digital continuity statement:

- A statement of purpose and requirements for keeping the records
- The names of the individuals responsible for long term data preservation
- A description of the information assets to be covered by the digital preservation statement
- A description of when the record needs to be captured into the approved file formats
- A description of the appropriate supported file formats for long-term preservation
- A description of the retention of all software specification information and licence information
- A description of how access to the information asset register is to be managed in accordance with the GDPR

13. Information audit

13.1. The alliance conducts information audits on an annual basis against all information held by the school to evaluate the information the school is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:

- Paper documents and records
- Electronic documents and records
- Databases
- Microfilm or microfiche
- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information

13.2. The information audit may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information and information flows, etc.
- Questionnaires to key staff members to identify information and information flows, etc.
- A mixture of the above

13.3. The DPO is responsible for completing the information audit. The information audit will include the following:

- The school's data needs
- The information needed to meet those needs
- The format in which data is stored
- How long data needs to be kept for
- Vital records status and any protective marking
- Who is responsible for maintaining the original document

13.4. The DPO will consult with staff members involved in the information audit process to ensure that the information is accurate.

13.5. Once it has been confirmed that the information is accurate, the DPO will record all details on the school's Information Asset Register.

13.6. The information displayed on the Information Asset Register will be shared with the headteacher to gain their approval.

14. Disposal of data

14.1. Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.

14.2. Where disposal of information is outlined as secure disposal, this will be disposed of by an approved third party securely and documented and electronic information will be scrubbed clean and, where possible, cut. The DPO will keep a record of all files that have been destroyed.

14.3. Where the disposal action is indicated as reviewed before it is disposed, the DPO will review the information against its administrative value – if the information should be kept for administrative value, the DPO will keep a record of this.

14.4. If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.

14.5. Where information has been kept for administrative purposes, the DPO will review the information again after three years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every three subsequent years.

14.6. Where information must be kept permanently, this information is exempt from the normal review procedures

15. Monitoring and review

15.1. This policy will be reviewed on an annual basis by the DPO in conjunction with the headteacher – the next scheduled review date for this policy is September 2019.

15.2. Any changes made to this policy will be communicated to all members of staff and the governing board.