Information Recording, Reporting and Retention Policy

Approved by:	Penny Harris (Director) Jane Cox (Director)	**Date:** 1st September 2025
Last reviewed on:	1st September 2024	
Next review due by:	1st September 2026	

All policies are generated and reviewed with an awareness of equality and diversity in relation to pupils, staff and visitors and place safeguarding and wellbeing at the heart of all that we do.

Aims:
This policy aims to:

- Set out how pupils files, including child protection files, should be set up and managed either cloud or paper based
- Set out how incidents, behaviours and concerns relating to pupils should be reported and recorded
- To set out how pupil related communications and contact is recorded
- Set out how the school will manage information in line with current legislative frameworks

Responsibilities:
The school leader is responsible for implementation of this policy. All staff are responsible for accurate and timely information reporting and recording in line with this policy.

Pupil Files:
Pupils files are created for each pupil on admission to the school. These can be held in secure paper files, on the school's information management system (MIS), the MyConcern platform and on the school's cloud storage. Each new pupil must be entered on the Admissions Register, on their first day, and their full profile recorded on the MIS.

Information that will be recorded and stored is:

- Admissions documentation
- EHCP plans, reviews and related documentation
- Personal Learning Plans
- Reports
- Baseline Assessments and progress tracking data
- Accreditation and examination results
- All communication and meetings relating to the pupil
- Attendance records

- Behaviour Daybooks (including incidents)
- Behaviour and Relational Support Plans
- MyConcern forms
- Success forms
- Suspension documentation
- Medication records

Child Protection Files:
If a pupil has had a child protection file at another school, this will be transferred to the new school either as a paper file or an electronic file. If a file does not arrive the School Leader must establish that such a file did not exist at the previous school.

All child protection files must be kept securely.

If a safeguarding concern is raised for a pupil at the school, whom does not already have a child protection file, then one must be set up on the MyConcern platform.

Any child protection file should contain all ongoing safeguarding information including:

- All communications
- Meeting notes
- All actions
- Incident reports
- Safeguarding concern forms
- Previous CP file information

If a Child Protection file is created, a red circle should be placed in the top right hand corner of any other paper based file/folder to indicate the existence of a Child Protection file. Cloud based files will be marked as child protection included.

Cloud based or MyConcern files should:

- Only be accessible by senior leaders and members of the child protection team
- Be set up with 2 factor authentication
- Not be left open on computer screens
- Be transferred securely to a pupil's new school if they leave

Paper based child Protection files should:

- Be kept in a locked filing cabinet in a room that is also locked if a staff member is not present
- Not be left open or unattended
- Identified on the exterior by first name and pupil admissions number
- Only contain relevant information
- Be transferred securely to a pupil's new school if they leave

Incident, Behaviour and Concern Reporting
It is a legal requirement and responsibility for school staff members to accurately report behavioural events in order for preventative measures to be put in place to stop a reoccurrence. Incidents should be recorded within 24 hours of the event. All staff witnesses should contribute to each report.

Behaviour Daybooks classified as incidents should be written to report the most serious of events, such as one which will almost certainly lead to suspension and possibly result in police involvement.
The content of these forms must be completely factual. Relevant commissioners should be informed within 48 hours.

Examples of events that should be recorded as an *incident* include, but are not limited to:

- Violence causing harm
- Use of physical intervention

- Lighting a fire
- Self-harm
- Discrimination or prejudice

Behaviour Daybook forms should be used to report behavioural events that do not meet the threshold of an incident; they must be classified as an Incident if they meet this threshold.

Examples of events that should be recorded as a *behaviour* include, but are not limited to:

- Low level violence with no harm caused
- Damage to property
- Obstructive behaviour
- Refusal to follow instructions
- Use of abusive language

All incident and behavioural daybooks should be completed factually, with as much detail as possible.

Using the MyConcern platform, safeguarding concerns should be written to record information about a pupil that gives reasons to be concerned. All concerns should be reported, even if the concern has been reported elsewhere or previously. Actions, as a result of a concern being reported, should be recorded.

Contact and Communication Records

All communications relating to pupils must be recorded on either a Contact or Meeting daybook on the school's MIS. This includes, but is not limited to, records of:

- Phone calls
- Emails
- Text and other messages
- Meetings

Records of communications are held on the MIS. If the communication relates in any way to child protection or safeguarding it is included on the MyConcern platform.

Complaints Log

The school must keep a secure record of all formal complaints, in relation to a pupil, including the following information:

- Date received
- How the complaint was received
- Who the complaint was received from
- Brief details of the complaint
- How the complaint was resolved
- Action taken by the school as the result of the complaint

This record must be made available to Ofsted or the Secretary of State on request.

Retention and Destruction of Information

Once records have reached the end of their administrative life, they should be disposed of in the appropriate way.

The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction. Members of staff should record at least:

- File reference (or other unique identifier);
- File title (or brief description);
- Number of files
- The name of the person authorising destruction of the information

The record of file destruction should be kept securely and backed up regularly offsite (on the school's cloud storage).

Please be aware that this guidance applies to all types of record, whether they are in paper or digital format.

- Paper records should be shredded using a cross-cutting shredder
- CDs / DVDs should be cut into pieces
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded
- Hard Disks should be dismantled and sanded

There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way. Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider should have been trained in the handling of confidential documents.

ADMINISTRATIVE		
Basic file description	*Retention Period*	*Action to be taken*
Daybook forms: • Incident • Physical Intervention • Suspensions	Date of last entry + 6 years then review	Secure disposal
Complaints log book and file	Date of resolution of complaint + 6 years	Secure disposal
Minutes of staff meetings	Date of meeting + 3 years	Secure disposal
School Development Plans	Life of plan + 3 years	Secure disposal
Admissions Registers	Every entry in the admissions register must be preserved for a period of three years after the date on which the entry was made.	Secure disposal
Attendance Registers	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	Secure disposal
Offsite registers	Current year + 1 year	Secure disposal
Offsite and trip risk assessments	Life of risk assessment + 3 years	Secure disposal
Visitors Book	Current year + 6 years	Secure disposal
Newsletters	Current year + 1 year	Standard disposal
Keyworking records	Current year + 1 year	Secure disposal

HEALTH AND SAFETY		
Basic file description	*Retention Period*	*Action to be taken*
Fire precaution log books	Current year + 6 years	Secure disposal
Health and Safety Risk Assessments	Life of risk assessment + 3 years	Secure disposal
Records relating to an accident at work (can be sent to HR Office or kept on file at the school)	Date of incident + 12 years	Secure disposal
Accident reports relating to adults	Date of incident + 6 years	Secure disposal
Accident reports relating to children	Date of birth + 25 years	Secure disposal
COSHH records	Current year + 40 years	Secure disposal
Asbestos management and monitoring records	Current year + 40 years	Secure disposal

PUPIL		
Basic file description	*Retention Period*	*Action to be taken*
Pupils files and folders to include: • Admissions paperwork • EHC Plans	Date of birth + 25 years	Secure disposal

• Report e.g. Educational Psychology • Annual review paperwork • Risk Assessments and Relational Support Plans • Pupil related communications • Medication Records (An individual pupil's files and folders can be merged during archiving)		
Child Protection Files and MyConcern data	Date of birth + 25 years	Secure disposal

HR		
Basic file description	*Retention Period*	*Action to be taken*
Application forms/interview notes for **unsuccessful** candidates (including information contained in emails)	Date of appointment of successful applicant + 6 months	Secure disposal
DBS Certificates	If a copy is taken, do not retain for longer than 6 months	Secure disposal
Staff personnel files (if held on the school site, transfer all records to HR Office on termination of employment)	Termination of employment + 6 years **UNLESS** Allegation of a child protection nature against a member of staff including where the allegation is unfounded: Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then review. Note: allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned.	Secure disposal
APR documentation (transfer records to HR Office on termination of employment)	Current year + 5 years	Secure disposal

TEACHING AND LEARNING		
Basic file description	*Retention Period*	*Action to be taken*
Exam results (school copies)	Current year + 6 years	Secure disposal
Pupils work	Current year + 1 year (if not returned to pupil)	Standard disposal
Teaching / Assessment records	Current year + 1 year	Standard disposal
Schemes of work	Current year + 1 year	Standard disposal

Review

In order to ensure that this policy is relevant, if you have any comments please email directors@ontrackeducation.com