



St. Anne's School

Data Protection and

Retention Policy

2025 2026

Context for Data Protection and Retention

On May 25th 2018, new legislation developed by the Council of the European Union came into force. This is known as GDPR (General Data Protection Regulation). The aim of GDPR is to:

- Strengthen and unify data protection for all EU citizens
- Give back control over personal data to EU citizens and residents
- Create new 'digital rights' for EU citizens
- Simplify and unify regulation within the EU
- Make it easier for non-EU countries to comply with their regulations.

General Data Protection Regulation is therefore a ground-breaking privacy law that regulates how **personal data** is collected, handled and protected. GDPR legislation aims to ensure that personal data is processed responsibly. GDPR places responsibilities on school as **data processors**. Schools hold personal data of students, parents/guardians and also staff members.

Data Subject is a living individual who can be identified, directly or indirectly from the personal data which is being processed

Personal Data is any information which relates to an identified or identifiable natural person (data subject); such as name, an identification number, address, an online identifier or to one or more factors specific to, for example the physical, economic, cultural or social identity of that natural person.

Special Category Personal Data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health or a person's sex life or sexual orientation.

Processing Data refers to any operation or set of operations performed on personal data, such as collection, recording, storage, and alteration, disclosure by transmission, dissemination or otherwise making available, erasure or destruction.

DPIA – Data Protection Impact Assessment and Data Sharing Agreements.

Data Protection Impact Assessment is a process which identifies risks arising out of the processing of personal data. These DPIA's are important tools for identifying risks and demonstrating compliance with GDPR.

Data Sharing Agreement is a contract between the school and another entity processing data on behalf of the school or where a school is involved with other services and ensures appropriate

technical and organisational measures are implemented and that processing complies with the applicable data protection legislation.

Article 9 relates to the processing of **Special Category Personal Data** and is prohibited except in limited circumstances set out in **Article 9 of the GDPR**.

Rationale

A policy on data protection and record keeping is necessary to ensure that the school has proper procedures in place in relation to accountability and transparency. It is good practice to record pupil progress so as to identify learning needs. A policy must be put in place to ensure a school complies with legislation such as:

- Education Act, Section 9g requiring a school to provide access to records to students over 18/parents
- Education Welfare Act – requiring a school to report school attendance and transfer of pupils
- GDPR Legislation 2018 which includes amendments to previous legislation
- Data Protection Act 2018

Relationship to School Ethos

St. Anne' School promotes openness and co-operation between staff, parents and pupils as a means towards providing the caring environment through which a child can develop and grow to his/her full potential. This policy was formulated by Staff and Board of Management of St. Anne's School. The purpose of the policy is to identify the records required to be retained by the school and to ensure confidentiality and manageable procedures in relation to access to such records by parents and stakeholders.

Aims/Objectives

- To ensure the school complies with legislative requirements
- To clarify the types of records maintained and the procedures relating to making them available to the relevant bodies
- To put in place a proper recording and reporting framework on the educational progress of pupils
- To establish clear guidelines on making these records available to parents and past pupils who are over 18
- To stipulate the length of time records and reports will be retained.

Guidelines

The Principal assumes the function of data controller and supervises the application of the Data Protection Act within the school. The data under the control of the Principal comes under the following headings.

1. Personal Data:

This data relates to personal details of the students such as name, address, date of birth, gender, ethnic origin, nationality, religious belief, medical details, dietary information, PPSN, contact details and parents/guardian's names. This information is included in the School Enrolment Form. These forms are kept in the Principal's Office. Information such as name, address, contact numbers and registration numbers on pupils are stored in both hard and soft copy format.

2. Student Records:

Student records are held by each class teacher in a locked filing cabinet or assessment folder.

Student records may contain:

- Personal details of the student
- Copy of medical sensitive data
- Copy of Psychological Assessment
- Copy of consent forms
- School report cards
- Teacher-designed tests.
- Standardised Tests
- Attendance Records

- Diagnostic Tests
- Photographs
- Samples of pupil's work
- Reports from CDNT, Clare Crusaders and Private Therapists
- Student Support Plan/Personal Pupil Plan
- Details of behavioural incidents or accidents

The following records are stored securely in the Principal's Office

- Psychological Assessments
- Medical sensitive data
- Consent forms
- Assessment results carried out by professionals to assist teaching and learning (e.g. results of psychiatric reports; occupational therapy reports; speech and language assessments; etc).
- Standardised Test Results
- Student Support Plan/Personal Pupil Plan
- Child Protection concerns and HSE referrals
- Minutes of HSE Child Protection Conferences.
- Incident and accident report forms

3. Staff Data

Staff records include name, address, contact details, payroll number, PPSN, qualifications, records of interview procedures, results of interview process, Interview board recommendations to BOM, BOM recommendations to Bishop, contracts, pension details, references, curriculum vitae, job applications, attendance records, Teaching Council registration, Garda Clearance, Statutory Declaration where necessary, Medical Fitness to Teach. Access is restricted to the Principal and Secretary. Records are destroyed by way of shredding when no longer required. These records are kept in the Principal's office. Attendance details are recorded on the OLCS system, are password protected and are accessed by the Secretary, the Principal, and the Chairperson of the Board of Management if necessary.

4. Administrative Data:

- Attendance Reports, Aladdin, POD, Registers
- Correspondence between parents and teachers
- Accident Report Book
- Administration of Medicines Indemnity Form
- Policies
- Records of physical intervention, records of incidents and records of allegations/ incidents of bullying and alleged bullying (manually recorded notes) (kept in Principal's Office)
- Records kept in line with Children First Procedures (Child Protection) (kept in Principal's Office)
- Accounts

Board of Management records:

These include:

- Name, address and contact details of each member of the Board of Management.
- Records in relation to appointments to the Board
- Minutes of Board of Management meetings and correspondence to the Board which may include references to particular individuals.
- Minutes, reports and correspondence relating to the Board of Management are kept in the Principal's office. Child Protection matters reported to the Board will not identify a pupil by name except in exceptional circumstances.

Access to Records:

Subject to consent, the following will have access where relevant and appropriate to the data listed above:

- Parents/Guardians
- Past Pupils over 18
- Health Service Executive staff
- National Educational Psychological Service
- Tusla – Child and Family Agency
- Therapists working with pupils
- Designated School Personnel
- Department of Education and Skills (where necessary)
- First and Second level schools (where relevant)
- St. Anne's School Board of Management

Parental authorisation must be provided by parents in the event of data being transferred to outside agencies such as health professionals, etc.

Outside agencies requesting access to records must do so in writing giving seven days' notice. Parents/guardians can make such a request either by phone, email or in writing. The right to erasure or rectification is available to change any mistakes or inaccuracies by proper authorisation through the same procedures. A standardised school report form is sent to the parents in line with relevant school policies.

Storage and Data Retention:

All records deemed 'never to be destroyed' are stored in the school office in a locked filing cabinet designated 'archives'.

A pupil profile and selection of records are held by each teacher in his/her individual classroom and passed on to the next teacher as the child moves to the next class.

All completed school roll books are stored in a similar location in addition to samples of children's work and pupil profiles.

Access to these stored files is restricted to authorised personnel only.

For computerised records, systems are password protected.

Responsibilities

The Principal assumes the function of data controller and supervises the application of the Data Protection Act within the school.

Board of Management

The BoM implement appropriate technical and organisational measures and should be able to demonstrate that data processing is performed in accordance with the Regulation; review and update those measures where necessary considering at all times (with regard to the processing of personal data)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

In addition:

- Review and approve the Data Protection Policy
- Supporting the Principal in the implementation of this policy
- Review the implementation, effectiveness and compliance with policies, procedures and protocols
- Ensure Data Protection is an Agenda item at BoM meetings where appropriate
- Ensuring that personal data discussed at Board of Management Meetings is kept secure at all times
- Any data on paper is handed back to the Principal at the end of each BoM Meeting.

Principal and Deputy Principal:

- Ensure the policy is communicated throughout the school
- Ensure the policy is implemented throughout the school
- Ensure personal data relating to students and staff is collected and processed in accordance with this policy
- Ensure that the basic principles of data protection are explained to staff and parents/guardians
- Ensure that there are regular updates to data protection awareness, so that data protection is a 'living' process aligned to the school's ethos
- Periodically check data held regarding accuracy
- Driving privacy and data protection awareness in the school
- Identifying training needs and arranging for refresher training sessions
- Escalating appropriate issues to the Board of Management

- Taking appropriate preventative actions to mitigate the risk of data breaches arising
- Spearheading the response to any data breach (following the data breach protocol)
- Due diligence of service providers (data processors) prior to any service provider being retained
- Ensuring adequate assurances of GDPR compliance are obtained
- Ensuring appropriate contracts in place with all service providers
- Ensure that record-keeping of data protection items is carried out
- Ensure BoM Minutes and records are kept secure in locked filing cabinets at all times
- Ensure that electronic versions of BoM Minutes are kept secure in password protected devices
- Ensure minutes that identifies vulnerable persons or particularly sensitive data is anonymized where possible
- Ensure that information is kept secure at all times and that the information is shredded as soon as could be reasonably expected
- Periodic reviews of all data protection arrangements are carried out.

Staff

- Read and confirm acknowledgement of this policy
- Adhere to the values and standards set forth in this policy and comply with relevant school procedures
- Request clarification if there is uncertainty
- Check that any information that you provide in connection with their employment is accurate and up to date
- Adherence to high standards of ethics and professionalism in all data entries (e.g. when entering notes about a student on any system)
- Ensure personal data is kept safe and secure, and is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party
- Ensure personal data related to students is accurately processed in accordance with this policy
- Ensure personal data (particularly sensitive personal data) is never brought offsite unless appropriate steps are taken to protect the data in motion (e.g. if taking personal data to a TUSLA case conference to review a child, ensure the data are stored securely on an encrypted laptop)
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data
- Assisting the Principal with access requests.

Data Breach Action Plan

A **Data Breach** refers to the “accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data”.

Procedure to follow for a Data Breach:

- Identify and confirm volumes and types of data affected
- Establish what personal data is involved in the breach
- Identify the cause of the breach
- Estimate the number of data subjects affected
- Establish how the breach can be contained.

Containment and Recovery:

- Establish who within the school needs to be made aware of the breach
- Establish whether there is anything that can be done to recover the losses and limit the damage the breach could cause
- Consider partial or complete systems lockdown
- Establish if it is appropriate to notify affected individuals immediately (for example where there is a high level of risk of serious harm to any individual).

Risk Assessment

Assessment of volumes and types of data involved will be undertaken and a risk assessment carried out to establish and the risk to data subjects

Notification

On the basis of the evaluation of risks and consequences, the Principal will decide whether it is necessary to notify relevant stakeholders i.e.:

- the Gardaí
- the Data Subjects affected by the breach
- the Data Protection Commissioner
- the school’s Insurers.

In accordance with the Data Protection Commissioner’s Code of Practice all incidents in which Personal Data has been put at risk will be reported to the Office of the DPC by the Principal within 72 hours of the school first becoming aware of the breach. If, following the assessment described above, it is established that the data breach has been fully and immediately notified to the Data Subjects affected and it affects no more than 100 Data Subjects and it does not include sensitive personal data or personal data of a financial nature, it may not be required to

be notified to the DPC. This will be assessed on an individual basis according to the school's policy on the data breach as above, and where there is any doubt, legal advice will be sought.

Evaluation and Response

Following any serious breach of data incident, a thorough review will be undertaken by the school and a report will be made to the Board of Management. This will identify the strengths and needs of the process and will indicate what areas may need to improve. A response may also include updating the Data Protection Policy and retraining staff.

Success Criteria

- Compliance with Data Protection Act and Statute of Limitations Act
- Easy access to records
- Framework in place for ease of compilation and reporting
- Manageable storage of records.

Roles and Responsibilities

The school staff, under the direction of the Principal will implement and monitor this policy. The principal has given an overview to staff at a staff meeting, in relation to each individuals' obligations in relation to data protection and retention. Individual teachers will design, administer and record all in-class testing. The principal will ensure that the storage for records is maintained and available for staff to use in line with current recommendations. If any further equipment for storage is necessary, staff should bring this to the attention of the principal.

Support for Schools

Data Protection Officer in NABMSE. The role has primary responsibility for ensuring that all special schools and NABMSE member schools are compliant with current and future data protection regulation.

The role is also:

- To ensure that special schools are compliant with GDPR and oversee all aspects of data management and data protection governance
- To develop data and information compliance business processes with a focus on the EU General Data Protection Regulation (GDPR) and related Data Protection legislation.
- To lead the development, implementation and maintenance of data retention and retrieval policies and procedures.
- Prepare and deliver data protection training to school staff.
- To act as a point of contact for members on data protection enquiries and for the Data Protection Commissioner.
- To oversee/supervise all work required to ensure and maintain GDPR compliance, including advice and monitoring all aspects of data privacy across special schools.
- To develop an appropriate data audit process.

Other supports for schools can be found at: <https://gdpr4schools.ie/>

Implementation Date

This new policy is effective from 8th October 2025.

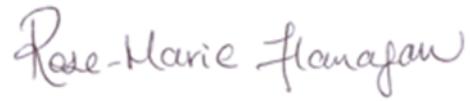
All records held from before that date will continue to be maintained in the school.

Review/Ratification/Communication

This policy was ratified on 8th October 2025.



Beth Hickey, Chairperson



Rose-Marie Flanagan, Secretary

The policy will be available on the school website and through the office.

It will be reviewed annually and amended if necessary.

Appendix

Data Retention Schedule

Student Records	Final Disposition	Retention Comments
Registers/Roll books/Aladdin	N/A	Indefinitely. Archive when class leaves + 2 years
State exam results	N/A	SEC responsibility to retain, not a requirement for the school to retain.

Records relating to pupils/students	Final Disposition	Retention Comments
Enrolment Forms (for pupils admitted to the school)	N/A	Indefinitely
Pupil transfer forms (Applies from one school to another)	N/A	Indefinitely
In-school standardised test results & SEN assessments	N/A	Indefinitely
End of term/year reports	N/A	Indefinitely
Disciplinary notes	N/A	Never destroy
School tours/trip records (including permission slips, itinerary reports)	N/A	Never destroy
Sensitive Personal Data Students	Final disposition	Retention Comments
Section 29 appeal records (for pupils enrolled in the school)	N/A	Never destroy
Accident/incident reports	N/A	Never destroy
Records of complaints made by parents/guardians	Confidential shredding or N/A, depending on the nature of the records	If it is child-safeguarding, a complaint relating to teacher-handling, or an accident, then retain indefinitely. Never destroy.
Enrolment forms where child not enrolled/ refused enrolment	Confidential shredding/ deletion	Two years after non-admission, to provide time for review/appeal process
Psychological assessments	N/A	Never destroy
SEN files, reviews, correspondence & Student Support Plans	N/A	Never destroy
Child protection records	N/A	Never destroy

Staff personnel files (whilst in employment)	Final Disposition	Comments
e.g. applications, qualifications, references, recruitment, job specification, contract, Teaching Council registration, staff training records etc.	Confidential shredding. Retain an anonymised sample for archival purposes.	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Application &/CV	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Qualifications	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
References	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Interview: database of applications (section which relates to employee only)	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Selection criteria	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Interview board marking scheme & board notes	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Interview board panel recommendation	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Recruitment medical	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Garda Vetting outcome	Confidential shredding/ deletion	Record of outcome retained for 12 months. School to retain reference number & disclosure date on file, which can be checked with An Garda Síochána in the future.
Job specification/ description	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Contract/Conditions of employment	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Probation letters/forms	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
POR applications & correspondence	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)

Allegations/complaints	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school). Please note relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains “active” on an employee’s record.
Grievance and Disciplinary records	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school). Please note relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains “active” on an employee’s record.
Leave of absence applications	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Job share	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Career break	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Maternity leave	Confidential shredding/ deletion	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Paternity leave	Confidential shredding/ deletion	Retain for 2 years after retirement/ resignation or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater).
Parental leave	Confidential shredding/ deletion	Must be kept for 8 years – Parental Leave Act 1998. Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater).
Parent's leave	Confidential shredding/ deletion	Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater).
Force Majeure leave	Confidential shredding/ deletion	Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater).
Carers Leave	Confidential shredding/ deletion	Must be kept for 8 years – Carer’s Leave Act 2001. Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater).
Working Time Act (attendance hours, holidays, breaks)	Confidential shredding/ deletion	Retain for 3 years or the duration of employment plus 7 years (6 years in which to take a claim against the school,

		plus 1 year for proceedings to be served on the school) (whichever is the greater).
Recruitment Process Unsuccessful Candidate Records	Final disposition	Comments
Note: these retention periods apply to unsuccessful candidates only.		
Candidate applications/ CVs called for interview	Confidential shredding / deletion	18 months from close of competition: 12 months plus 6 months for Workplace Relations Commission to inform school that claim is being taken.
Database of applications	Confidential shredding / deletion	18 months from close of competition: 12 months plus 6 months for Workplace Relations Commission to inform school that claim is being taken.
Selection criteria	Confidential shredding / deletion	18 months from close of competition: 12 months plus 6 months for Workplace Relations Commission to inform school that claim is being taken.
Applications of candidates not shortlisted	Confidential shredding / deletion	18 months from close of competition: 12 months plus 6 months for Workplace Relations Commission to inform school that claim is being taken.
Unsolicited job applications	Confidential shredding / deletion	18 months from close of competition: 12 months plus 6 months for Workplace Relations Commission to inform school that claim is being taken.
Candidates shortlisted but unsuccessful at interview	Confidential shredding / deletion	18 months from close of competition: 12 months plus 6 months for Workplace Relations Commission to inform school that claim is being taken.
Successful candidates who do not accept offer	Confidential shredding / deletion	18 months from close of competition: 12 months plus 6 months for Workplace Relations Commission to inform school that claim is being taken.
Interview board marking scheme & board notes	Confidential shredding / deletion	18 months from close of competition: 12 months plus 6 months for Workplace Relations Commission to inform school that claim is being taken.
Panel recommendation by interview board	Confidential shredding / deletion	18 months from close of competition: 12 months plus 6 months for Workplace Relations Commission to inform school that claim is being taken.

Occupational Health Records	Confidential Shredding	Comments
Sickness absence records/certificates	Confidential shredding Or do not destroy	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/injury/ incident sustained in relation to/in connection with an individual's school duties, in which case, do not destroy.
Pre-employment medical assessment	Confidential shredding Or do not destroy	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/injury/ incident sustained in relation to/in connection with an individual's school duties, in which case, do not destroy.

Occupational health referral	Confidential shredding Or do not destroy	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to/in connection with an individual's school duties, in which case, do not destroy.
Correspondence re retirement on ill-health grounds	Confidential shredding Or do not destroy	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to/in connection with an individual's school duties, in which case, do not destroy.
Medical assess/ referrals	Confidential shredding Or do not destroy	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to/in connection with an individual's school duties, in which case, do not destroy.
Sick leave records (sick benefit forms)	Confidential shredding Or do not destroy	In the case of audit/refunds retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to/in connection with individual's school duties, in which case, do not destroy.
Accident/injury reports	Confidential shredding Or do not destroy	Retain for 10 years or the duration of the employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to/in connection with individual's school duties, in which case, do not destroy.

Government Returns	Final Disposition	Comments
Any returns which identify individual members of the school community	Confidential shredding/ retained indefinitely	Depends on return. If it relates to pay/pension/benefits of staff, keep indefinitely as per DE guidelines. If it relates to student information, e.g. October Returns, Annual Census etc., "Student Records" guidelines apply.

Superannuation /Pension /Retirement records	Final Disposition	Comments
Records of previous service (incl. prev. correspondence)	N/A	DE advises that these should be kept indefinitely.
Pension calculation	Confidential shredding/ deletion	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/ former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school whichever longer)
Pension increases	Confidential shredding/ deletion	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/ former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school whichever longer)

Salary claim forms	Confidential shredding/ deletion	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/ former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school whichever longer)
--------------------	----------------------------------	--

Board of Management Records	Final Disposition	Comments
Board agenda and minutes	N/A	Indefinitely. Store securely on school property
Principal's monthly report including staff absences	N/A	Indefinitely. Administrative log and does not relate to any one employee in particular: the monthly reports are not structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. Not a "relevant filing system".
School closure	Transfer	On school closure, school to liaise with Patron. decommissioning exercise should take place with respect to archiving and recording data.

Financial Records	Final Disposition	Comments
Payroll and taxation	Confidential shredding/ retained indefinitely	Revenue Commissioners require records be kept for at least 6 years after the end of the tax year. Records must be made available for inspection by authorised Revenue Commissioner officers or of Dept. of Social Protection. Note: The DE requires schools that "pay, taxation and related school personnel service records should be retained indefinitely within the school. These records can be kept either on a manual or computer system.
Audited accounts	N/A	Indefinitely
Invoices/ back-up records/ receipts	Confidential shredding/ deletion	Retain for 7 years