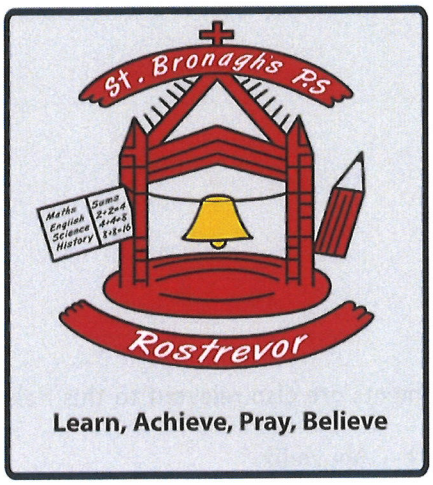
St Bronagh's PS



Data Protection Policy

Date Ratified by BOG: 8/11/23

Review Date: Autumn 2025.

Signed: _____

Chair of Board of Governors

EXECUTIVE STATEMENT

At St Bronagh's Primary School, we believe privacy is important. We are committed to complying with our data protection obligations and to being concise, clear and transparent about how we obtain and use Personal Information and how (and when) we delete that information once it is no longer required.

We will review and update this Data Protection Policy regularly in accordance with our data protection obligations.

Any queries in relation to this policy or any of the matters referred to in it should be submitted to the Principal at jgallagher844@c2kni.net or at -

St Bronagh's PS,

53, Church Street,

Rostrevor,

Co Down,

BT34 3BB.

The following policies, procedures and documents are also relevant to this Policy:

- Data Breach Management Procedure – Appendix 1
- Subject Access Request Procedure – Appendix 2
- Department of Education Document Disposal Schedule – Appendix 3

DATA PROTECTION POLICY

1. Scope

1.1. The School is subject to the General Data Protection Regulation (GDPR) which imposes obligations on the School as a data controller in relation to the protection, use, retention and disposal of Personal Information. This Policy sets out the procedures that are to be followed when dealing with Personal Information and applies to all Personal Information processed by or on behalf of St Bronagh's Primary School.

1.2. You must read this Policy because it gives important information about:

1.2.1. the data protection principles with which St Bronagh's Primary School must comply;

1.2.2. what is meant by Personal Information and Special Category Data;

1.2.3. how we gather, use and (ultimately) delete Personal Information and Special Category Data in accordance with the data protection principles;

1.2.4. where more detailed Privacy Information can be found, e.g. about the Personal Information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;

1.2.5. your rights and obligations in relation to data protection; and

1.2.6. the consequences of our failure to comply with this Policy.

1.3. Please refer to the School's privacy notices on our website www.stbronaghs.org and, where appropriate, to other relevant policies including our eSafety Policy, which contain further information regarding the protection of Personal Information in those contexts.

2. Data Protection Principles

2.1. GDPR sets out the following principles with which any party handling Personal Information must comply. All Personal Information must be:

2.1.1. processed lawfully, fairy and in a transparent manner;

2.1.2. collected for specified, explicit and legitimate purposes only, and will not be further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

2.1.3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

2.1.4. accurate and, where necessary, kept up to date and take reasonable steps to ensure that inaccurate Personal Information are deleted or corrected without delay;

2.1.5. kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the information is processed; Personal Information may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of the individual; and

2.1.6. processed in a manner than ensures appropriate security of the Personal Information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Lawful, Fair and Transparent Processing

3.1. The School will, before any processing of Personal Information starts for the first time, and then regularly while it continues:

3.1.1. process the Personal Information on at least one of the following bases:

3.1.1.1. **Consent:**

- the individual has given their express agreement to the processing of their Personal Information for one or more specific purposes;
- parental consent will be obtained for any child aged under 13 years old;

3.1.1.2. **Contractual**:

- the processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract;

3.1.1.3. **Legal Obligation**:

- the processing is necessary for compliance with a legal obligation to which the School is subject;

3.1.1.4. **Vital Interests**:

- the processing is necessary for the protection of the vital interests of the individual or another natural person; or

3.1.1.5. **Public Interest**:

- the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or

3.1.1.6. **Legitimate Interests**:

- the processing is necessary for the purposes of legitimate interests of the School or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the individual, in particular where the individual is a child.

3.1.2. except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

3.1.3. document our decision as to which lawful basis applies to help demonstrate our compliance with the data protection principles;

3.1.4. include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notices. The school's privacy notice can be found on our website at www.stbronaghs.org

3.1.5. where Special Category Data is processed, identify a lawful special condition for processing that information and document it; and

3.1.6. where criminal offence information is processed, identify a lawful condition for processing that information and document it.

4. Rights of the Individual

4.1. The GDPR states that individuals have the following rights in respect of the processing of their Personal Information:

4.1.1. **The right to be informed**:

4.1.1.1. The School will keep individuals informed of its processing activities through its privacy notices on our website www.stbronaghs.org

4.1.2. **The right of access**:

4.1.2.1. An individual may make a subject access request ("**SAR**") at any time to find out more about the Personal Information which the School holds on them. All SARs must be forwarded to the Principal jgallagher844@c2kni.net.

4.1.2.2. The School is required to respond to a SAR within one month of receipt but this can be extended by up to two months in the case of complex and/or numerous requests and, in such cases, the individual will be informed of the need for such extension. The School does not charge a fee for the handling of a straightforward SAR.

4.1.3. **The right to rectification**:

4.1.3.1. If an individual informs the School that Personal Information held by the School is inaccurate or incomplete, the individual can request that it is rectified.

4.1.4. **The right to erasure**:

4.1.4.1. An individual is entitled to request that the School ceases to hold Personal Information it holds about them.

4.1.4.2. The School is required to comply with a request for erasure unless the School has reasonable grounds to refuse.

4.1.5. **The right to restrict processing**:

4.1.5.1. An individual is entitled to request that the School stops processing the Personal Information it holds about them in certain circumstances.

4.1.6. **The right to data portability:**

4.1.6.1. An individual has the right to receive a copy of their Personal Information and use it for other purposes.

4.1.7. **The right to object:**

4.1.7.1. An individual is entitled to object to the School's processing of their Personal Information.

4.1.8. **Rights in relation to automated decision making and profiling:**

4.1.8.1. An individual has the right to challenge any decision that is made about them on an automated basis (subject to certain exceptions).

4.1.8.2. The School is also required to comply with certain conditions if it uses Personal Information for profiling purposes.

5. Data Protection Officer

5.1. A Data Protection Officer (DPO) is appointed who will monitor adherence to this policy. The school has appointed the EA as their DPO.

5.2. The DPO is required to have an appropriate level of knowledge.

6. Privacy by Design

6.1. The School has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process Personal Information will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

6.2. The data protection impact assessment will include:

6.2.1. Consideration of how Personal Information will be processed and for what purposes;

6.2.2. Assessment of whether the proposed processing of Personal Information is both necessary and proportionate to the purpose(s);

6.2.3. Assessment of the risks to individuals in processing the Personal Information;

6.3. What controls are necessary to address the identified risks and demonstrate compliance with legislation.

6.4. A data protection impact assessment is conducted by the Principal:

6.4.1. On every business process periodically, at least once a year and more frequently where the amount and/or sensitivity of Personal Information processed, dictates so;

6.4.2. As part of the project calendar admission requirements checklist;

6.4.3. At every high-impact change, and/or at the request of the Data Protection Officer.

7. Data Retention & Disposal

7.1. The longer that Personal Information is retained, the higher the likelihood is of the expiry date being exceeded. Retention expiration triggers may be connected to accidental disclosure, loss, theft and/or information growing stale.

7.2. Any Personal Information kept by the School is managed in accordance with the Department of Education Disposal of Records Schedule (https://www.education-ni.gov.uk/publications/disposal-records-schedule).

8. Data Breach

8.1. A data breach is any (potential) unintended loss of control over or loss of Personal Information within the School's environment. Preventing a data breach is the responsibility of all the School staff and its workforce.

8.2. Please refer to the School's Data Breach Management Procedure.

9. Third-Party Services and Subcontracting

9.1. The School may decide to contract with a third party for the collection, storage or processing of data, including Personal Information e.g. GL Assessment, Renaissance UK etc.

9.2. If the School decides to appoint a third party for the processing of Personal Information, this must be regulated in a written agreement in which the rights and duties of the School and of the subcontractor are specified. A subcontractor shall be selected that will guarantee the technological and organisational security measures required in this Policy, and provide sufficient guarantees with respect to the protection of the personal rights and the exercise of those rights.

9.3. The subcontractor is contractually obligated to process Personal Information only within the scope of the contract and the directions issued by the School.

10. Complaints

10.1. Complaints will be dealt with in line with the School's complaints policy which is available on our school website or from the main office on request.

10.2. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. The ICO's details are as follows:

The Information Commissioner's Office – Northern Ireland

3rd Floor
14 Cromac Place,
Belfast
BT7 2JB

Telephone: 028 9027 8757 / 0303 123 1114
Email: ni@ico.org.uk

11. Definitions

"consent"	is any freely given, specific and transparently, well-informed indication of the will of the individual, whereby the individual agrees that his or her Personal Information may be processed. Particular requirements about consent can arise from the respective national laws.
"Personal Information"	(sometimes known as "personal data") means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly — in particular, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

"processing"	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with Personal Information.
"Special Category Data"	(sometimes known as "sensitive personal data") means Personal Information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data and the processing of data concerning health or sex life

Appendix 1

Data Breach Management Procedure

Step 1: Containment and Recovery

1. The Data Protection Officer will ascertain the severity of the breach, whether any personal data is involved and whether the breach is still occurring.

2. If the breach is still occurring, the Data Protection Officer will establish what steps need to be taken immediately to minimise the effect of the breach and contain the breach from further data loss (e.g. alert C2K, restricting access to systems or close down a system etc.).

3. The Principal and/or Data Protection Officer will consider and implement appropriate steps required to recover any data loss where possible and limit damage caused (e.g. use of backups to restore data; changing passwords etc.)

4. The Data Protection Officer will inform the Chair of Governors if the severity and likely impact of the breach deems it necessary to inform the ICO of the breach. At the same time, depending on the nature of the breach, the Data Protection Officer may seek expert or legal advice and/or the Police if it is believed that illegal activity has occurred or likely to occur.

5. Where a significant breach has occurred, the Principal and/or Data Protection Officer will inform the ICO within 72 hours of the discovery of the breach (see Notifications below).

6. The decision taken as to the reasons why a data breach is either reported or not reported is documented by the Data Protection Officer.

7. All the key actions and decisions are fully documented and logged in our Data Security Breach Log.

Step 2: Assessment of Risk

Further actions may be needed beyond immediate containment of the data breach. To help the school determine the next course of action, an assessment of the risks associated with the breach is undertaken to identify whether any potential adverse consequences for individuals are likely to occur and the seriousness of these consequences. The Data Protection Officer will consider the points arising from the following questions:

1. What type and volume of data is involved?

2. How sensitive is the data? Could the data breach lead to distress, financial or even physical harm?

3. What events have led to the data breach? What has happened to the data?

4. Has the data been unofficially disclosed, lost or stolen? Were preventions in place to prevent access/misuse? (e.g. encryption)

5. How many individuals are affected by the data breach?

6. Who are the individuals whose data has been compromised?

7. What could the data tell a third party about the individual? Could it be misused regardless of what has happened to the data?

8. What actual/potential harm could come to those individuals? E.g. physical safety; emotional wellbeing; reputation; finances; identity theft; one or more of these and other private aspects to their life

9. Are there wider consequences to consider?

10. Are there others that might advise on risks/courses of action (such as banks if individual's bank details have been affected by the breach)?

Step 3: Notification of Breaches

If the severity and likely impact of the breach warrants notifying the ICO, then we will notify the ICO within 24 hours of becoming aware of the essential facts of the breach (through the ICO's online portal at https://report.ico.org.uk/security-breach/).

This notification will include at least:

- Our school name and contact details;
- The date and time of the breach (or an estimate);

- The date and time we discovered it;
- Basic information about the type of breach;
- Basic information about the personal data concerned.

As we undertake a full investigation of the details of the breach, within 3 days of the initial notification, we will further provide the ICO with full details of the incident, the number of individuals affected and its possible effect on them, the measures taken to mitigate those effects, and information about our notification to the individuals affected.

There may be instances when the nature of the breach and the individual(s) affected may necessitate notifying third parties such as regulatory bodies, agencies, professional bodies as part of the initial containment.

If the breach is likely to adversely affect the personal data or privacy of our pupils, parents/carers, staff and/or governors, we will notify them of the breach without unnecessary delay if we cannot demonstrate that the data was encrypted (or made unintelligible by a similar security measure). We will inform them of:

- The estimated date of the breach;
- A summary of the incident;
- The nature and content of the personal data;
- The likely effect on the individual(s);
- Any measures we have taken to address the breach;
- How those affected can mitigate any possible adverse impact.

Step 4: Evaluation and Response

When the school's response to a data breach has reached a conclusion, the Data Protection Officer will undertake a full review of both the causes of the breach and the effectiveness of the response. The full review is reported to SLT and the Board of Governors for information and discussion as soon as possible after the data breach has been identified.

If through the review, systematic or ongoing problems associated with weaknesses in internal processes or security measures have been identified as a cause of the data breach, then appropriate action plans will be drafted, actioned and monitored to rectify any issues and implement recommendations for improvements. The Board of Governors will be party to discussions regarding action plans and be able to monitor progress against the actions appropriately.

If a breach warrants a disciplinary investigation, legal advice will be sought through the Employing Authorities Human Resources channels.

Implementation of these Procedures

The Data Protection Officer will ensure that staff are aware of these procedures for reporting and managing data breaches. Data Protection training for all staff is mandatory, including new employees and all staff will undertake refresher training annually.

If staff have any queries or questions relating to these procedures, they should discuss this with the Principal and/or Data Protection Officer.

Complaints about our Data Breach Management Procedure

If an individual or Data Subject affected by a data breach believes that a data breach has not been dealt with properly, a complaint should be made to the school through our normal complaints procedure. If following the conclusion of the complaints procedure within the school, the individual or Data Subject is still dissatisfied, then a complaint can be made directly to the Information Commissioner's Office (ICO) at https://ico.org.uk/concerns.

Appendix 2

Data Subject Access Request Procedure

PURPOSE

The General Data Protection Regulations (GDPR) entitles individuals to request access to any personal data that St Bronagh's Primary School is holding about them. This is known as a Subject Access Request (SAR). This document outlines the procedures surrounding making and responding to a SAR.

A SAR is where an individual, using their rights under GDPR, makes a request for a copy of the personal data an organisation holds on them, or details of what data is held and its source. A SAR does not have to reference GDPR, the term "Subject Access Request" or any legislative rights.

PROCEDURES

Making a SAR

SARs can be made verbally, via email or in writing to Mr Gallagher, principal, at the address below;

St Bronagh's PS, 53, Church Street, Rostrevor, Co. Down, BT343BB;

Tel: 028 41738450;

Email: jgallagher844@c2kni.net

If a SAR is made verbally, then the requester will be asked to put their request in writing, in order to allow the school to understand the nature of the SAR and to verify the identity of the requester.

Where a request is received elsewhere in the school, the principal should be immediately informed so that he is able to deal with the request with no undue delay.

Once the request is received, the principal will confirm the identity of the requester and assess the scope of the request.

Confirming the Identity of the Requestor

Additional information may be requested to evidence the identity of the requester. This can be established by production of two or more of the following:

- Current passport
- Current driving licence
- Recent utility bill with current address
- Birth/marriage certificate
- Recent credit card or mortgage statement

If the school is not satisfied as to the identity of the requester, then the request will not be complied with, so to avoid the potential for an inadvertent data breach.

If a request is made by a person seeking the personal data of a data subject, and which purports to be made on behalf of that data subject, then a response must not be provided unless and until written authorisation has been provided by the data subject. The school will not approach the data subject directly, but will inform the requester that it cannot respond without the written authorisation of the data subject. Where consent cannot be obtained, or is denied, the principal will consider the reasons and the school's duty of care to both parties to decide whether to disclose the information.

Fee for Responding to Requests

The school will usually deal with a SAR free of charge, however, a fee may be charged in the following circumstances;

- Where a request is considered to be manifestly unfounded or excessive, or
- Where a repeat request for the same information is made.

If appropriate, the school will respond in writing stating their reasons for refusing to respond to request.

Process for dealing with a SAR

Once the identity of the data subject (or the right/authority to request the data where the data subject is not the requester) has been verified, the principal will begin the process of contacting the appropriate members of staff to collect and collate the information.

The principal will take all reasonable and proportionate steps to identify and disclose all data relating to the request.

In order to locate the correct information within the school, the principal may ask the requester to confirm exactly what information they are requesting, or where they believe the information may be stored.

Where the information contains reference to third parties, the principal will redact (blank out) the third parties. Where this is impossible and consent from the third party has not been received the information will not be disclosed.

The information provided in reply to a request must be that which the school holds (subject to any exemptions) at the time the request is received. However, the GDPR allows routine updating and maintenance of the data to continue between the date on which the request is received and the date when the reply is dispatched. This means that the information provided to the individual may differ from that which was held at the time when the request was received, but only as a result of normal processing. Data cannot be deleted.

The principal will ensure that the information disclosed is clear and technical terms are clarified and explained. The response will be provided in a written format, via email or letter, including an explanation of the types of data provided and whether, and as far as possible for what reasons, any data has been withheld.

Time Period for Responding to a SAR

The school has one month to respond to a SAR. This will run from the latter of;

- The date of the request;
- The date when any additional identification, or other information requested, is received; or
- Payment of any required fee.

The period of response may be extended by a further two calendar months in relation to complex requests. If it is decided that the request is sufficiently complex as to require an extension of the period for response, the principal will notify the requester within one calendar month of receiving the request, together with the reasons as to why this is considered necessary.

If a request is received during extended school holiday periods it may not be able to be responded to within the one-month response period. If receipt is taken during this period, the school will send out an initial acknowledgement of the request, followed by a further acknowledgement as soon as possible following the start of the next term setting out details of when a full response will be provided (not greater than one month into the new term).

Contacts & Complaints

Any enquiries regarding this procedure or the school's Data Protection Policies should be directed to the principal using the contact details listed on page 1 of this appendix.

Appendix 3

Document Disposal Schedule

1. Management & Organisation

Ref	Record	Minimum Retention Period	Action After Retention
1.1	Board of Governors – general correspondence	Current school year + 6 years	Destroy
1.2	BOG Meetings Minutes (master)	Current school year + 6 years	Offer to PRONI for Permanent Preservation
1.3	Senior Management Team-Meeting Minutes	Current school year + 6 years	Offer to PRONI for Permanent Preservation
1.4	Staff Meeting Minutes	Current school year + 6 years	Destroy
1.5	School Development Plan	Retain in school for 10 years from closure of Plan	Offer to PRONI for Permanent Preservation
1.6	School Policies	Retain while current. Retain 1 copy of old policy for 2 years after being replaced	Destroy
1.7	PTA – minutes and general correspondence	Current school year + 6 years	Destroy
1.8	Visitors Book	Current school year + 6 years	Destroy
1.9	Circulars to Staff, Parents and Pupils	Current school year + 3 years	Destroy
1.10	School Brochure or Prospectus	Current school year + 3 years	Destroy
1.11	Comments/Complaints	5 years after closing. Review for further retention in the case of contentious disputes	Destroy
1.12	Annual Report	Retain in school for 10 years from date of Report	Offer to PRONI for Permanent Preservation
1.13	School Fund	Current financial year + 6 years	Destroy
1.14	Emergency Planning/Business Continuity Plan	Until superseded	Destroy

2. Legislation and Guidance from DE, EA, CCMS etc.

Ref	Record	Minimum Retention Period	Action After Retention
2.1	Education (NI) Order	Until superseded	Destroy

2.2	Circulars, Guidance, Bulletins from DE, EA etc.	Until superseded	Destroy
2.3	Correspondence re: Statistical Returns to DE, EA etc.	Current financial year + 6 years	Destroy
2.4	DE Reports, Inspections	Until superseded	Destroy

3. Pupils

Ref	Record	Minimum Retention Period	Action After Retention
3.1	*Pupil Admission Data*		
3.1a	Applications for enrolment	3 years after enrolment	Destroy
3.1b	Transfer applications (Transfer Forms)	3 years after enrolment	Destroy
3.2	Pupil Attendance Information/Registers	Date of Register + 10 years	Offer to PRONI for Permanent Preservation
3.3	Pupil Education Records - School/Progress Reports etc.	Until pupil is 23 years old	Destroy
3.4	Pupil Education Records - School/Progress Reports etc. (Special Educational Needs)	Until Pupil is 26 years old	Destroy
3.5	Child Protection Information- Record of concerns where case was not referred to Social Services	10 years after last entry on file	Destroy
3.6	Child Protection Information- Social Services investigation outcome was unfounded or malicious	10 years after last entry on file	Destroy
3.7	Child Protection Information- Social Services investigation outcome was inconclusive, unsubstantiated or substantiated	Until pupil is 30 years old	Destroy
3.8	Disciplinary Action (Suspension/Expulsion)/Offences – bullying	Until pupil is 23 years old	Destroy
3.9	Disciplinary Action (Suspension/Expulsion)/Offences – bullying (Special Educational Needs)	Until pupil is 26 years old	Destroy
3.10	Timetables + Class Groupings	Retain while current	Destroy
3.11	Examination Results	Current school year + 6 years	Destroy
3.12	Careers Advice	Current school year + 6 years	Destroy
3.13	School Meals returns	Current financial year + 6 years	Destroy

3.14	Free Meals registers	Current financial year + 6 years	Destroy
3.15	School Trips – Financial & Administration details	Current financial year + 6 years	Destroy
3.16	School Trips-Attendance/Staff Supervision etc.	Current financial year + 6 years. In the case of an incident/accident involving a pupil, retain until pupil is 23 years old or 26 for a pupil with special educational needs	Destroy
3.17	Reports of Stolen/Damaged Items	Current financial year + 6 years	Destroy
3.18	Medical Records – records of pupils with medical conditions and details for the administration of drugs when necessary.	Until pupil is 23years old or in the case of a Special Needs Pupil, until 26 years old	Destroy

4. Staff

Ref	Record	Minimum Retention Period	Action After Retention
4.1	Staff Personnel Records (including, appointment details, training, staff development etc.)	7 years after leaving employment	Destroy
4.2	Interview notes and recruitment records	Date of interview + 6 months	Destroy
4.3	Staff Salary Records	7 years after leaving employment	Destroy
4.4	Staff Sickness Records (copies of Medical Certs)	Current school year + 6 years	Destroy
4.5	Substitute Teacher Records	Current school year + 6 years	Destroy
4.6	Substitute Staff Records-non teaching (cover for nursery assistants)	Current school year + 6 years	Destroy
4.7	Student Records-non teaching (e.g. nursery assistant students & pupils from schools on work experience)	Current school year + 6 years	Destroy
4.8	Student Teachers on Teaching Practice – student teacher progress	Current school year + 6 years	Destroy
4.9	Procedures for Induction of Staff	Until superseded	Destroy
4.10	Staff/Teachers' Attendance Records	7 years after leaving	Destroy
4.11	Staff Performance Review	7 years after leaving	Destroy

5. Finance

Ref	Record	Minimum Retention Period	Action After Retention
5.1	Annual budget and budget deployment	Current financial year + 6 years	Destroy
5.2	Budget Monitoring	Current financial year + 6 years	Destroy
5.3	Annual Statement of Accounts (Outturn Statement)	Current financial year + 6 years	Destroy
5.4	Order Books, Invoices, Bank Records, Cash Books, Till Rolls, Lodgement books etc.	Current financial year + 6 years	Destroy
5.5	Postage Book	Current financial year + 6 years	Destroy
5.6	Audit Reports	Current financial year + 6 years	Destroy

6. Health & Safety

Ref	Record	Minimum Retention Period	Action After Retention
6.1	Accident Reporting (Adults)	Date of incident + 7 years	Destroy
6.2	Accident Reporting (Children)	Until pupil is 23years old or in the case of a Special Needs pupil, until 26 years old	Destroy
6.3	Risk Assessments – work experience locations/pupils	7 years	Destroy
6.4	H & S Reports	15 years	Destroy
6.5	Fire Procedure	Until superseded	Destroy
6.6	Security System File	For the life of the system	Destroy