Introductory Statement

Headfort School's Data Protection Policy applies to the personal data held by the school's Trust which is protected by the Data Protection Acts 1988 to 2018 and the EU General Data Protection Regulation (GDPR).

The policy applies to all school staff, the Trust, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school) insofar as the measures under the policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation.

This policy sets out the manner in which personal data and special categories of personal data will be protected by the school. Headfort operates a **"Privacy by Design"** method in relation to Data Protection. This means we plan carefully when gathering personal data so that we build in the data protection principles as integral elements of all data operations in advance. We audit the personal data we hold in order to:

1. be able to provide access to individuals to their data
2. ensure it is held securely
3. document our data protection procedures
4. enhance accountability and transparency

Data Protection Principles

The school Trust is a *data controller* of *personal data* relating to its past, present and future staff, students, parents/guardians and other members of the school community. As such, the Trust is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 to 2018 and GDPR, which can be summarised as follows:

1. **Obtain and process Personal Data fairly:** Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the school, parents/guardians of students etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the school. All such data is treated in accordance with the Data Protection Acts and the terms of this Data Protection Policy. The information will be obtained and processed fairly.

2. **Consent:** Where consent is the basis for provision of personal data, (e.g. data required to Extras, photos/ videos or any other optional school activity) the consent must be a freely-given, specific, informed and unambiguous indication of the data subject's wishes. Headfort will require a clear, affirmative action e.g. ticking of a box/signing a document, completing a Google Form to indicate consent. Consent can be withdrawn by data subjects in these situations

3. **Keep it only for one or more specified and explicit lawful purposes:** The school will inform individuals of the reasons they collect their data and will inform individuals of the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times.

4. **Process it only in ways compatible with the purposes for which it was given initially** Data relating to individuals will only be processed in a manner consistent with the purposes for which it was gathered. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.

5. **Keep *Personal Data* safe and secure:** Only those with a genuine reason for doing so may gain access to the information. Personal Data is securely stored under lock and key in the case of manual records and protected with computer software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) are password-protected

6. **Keep Personal Data accurate, complete and up-to-date:** Students, parents/guardians, and/or staff should inform the school of any change which the school should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, the school will make all necessary changes to the relevant records. The principal may delegate such updates/amendments to another member of staff. However, records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change.

7. **Ensure that it is adequate, relevant and not excessive:** Only the necessary amount of information required to provide an adequate service will be gathered and stored.

8. **Retain it no longer than is necessary for the specified purpose or purposes for which it was given:** As a general rule, the information will be kept for the duration of the

individual's time in the school. Thereafter, the school will follow the DES guidelines on the storage of Personal Data relating to a student. In the case of members of staff, the school will follow the DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The school may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law. See School Record Retention table in Appendix 1.

9. **Provide a copy of their *personal data* to any individual, on request:** Individuals have a right to know what personal data/sensitive personal data is held about them, by whom, and the purpose for which it is held.

   The minimum age at which consent can be legitimately obtained for processing and disclosure of personal data under rules 1 and 3 above is not defined in the Data Protection Acts. However, guidance material published on the Data Protection Commissioner's website states the following:

   "As a general rule in the area of education, a student aged eighteen or older may give consent themselves. A student aged from twelve up to and including seventeen should give consent themselves and, in addition, consent should also be obtained from the student's parent or guardian. In the case of students under the age of twelve consent of a parent or guardian will suffice."

Scope

The Data Protection legislation applies to the keeping and processing of *Personal Data*. The purpose of this policy is to assist the school to meet its statutory obligations, to explain those obligations to School staff, and to inform staff, students and their parents/guardians how their data will be treated

The policy applies to all school staff, the Trust, parents/guardians, students and others (including prospective or potential students and their parents/guardians, and applicants for staff positions within the school) insofar as the school handles or processes their *Personal Data* in the course of their dealings with the school.

Definition of Data Protection Terms

In order to properly understand the school's obligations, there are some key terms which should be understood by all relevant parties.

Personal Data means any data relating to an identified or identifiable natural person i.e. a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller i.e. the school

Data Controller for the purpose of this policy is the Headfort Trust of Headfort School who delegate the responsibility for overseeing data protection on a day to day basis to the Headmaster.

Data Subject - is an individual who is the subject of personal data

Data Processing - performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data
- Retrieving, consulting or using the data
- Disclosing the data by transmitting, disseminating or otherwise making it available
- Aligning, combining, blocking, erasing or destroying the data

Data Processor - a person who processes personal information on behalf of a data controller, but **does not include an employee of a data controller** who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection legislation places responsibilities on such entities in relation to their processing of the data. i.e. Aladdin & School accounting/wages processors

Special categories of Personal Data refers to *Personal Data* regarding a person's

- racial or ethnic origin
- political opinions or religious or philosophical beliefs
- physical or mental health
- sexual life and sexual orientation
- genetic and biometric data
- criminal convictions or the alleged commission of an offence
- trade union membership

Personal Data Breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. This means any compromise or loss of personal data, no matter how or where it occurs

Rationale

In addition to its legal obligations under the broad remit of educational legislation, the school has a legal responsibility to comply with the Data Protection Acts 1988 to 2018 and the GDPR

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. The school takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the Headmaster and Trust to make decisions in respect of the efficient running of the School. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the school and the Trust

Other Legal Obligations

Implementation of this policy takes into account the school's other obligations and responsibilities. Some of these are directly relevant to data protection. The Trust has made the decision to follow the requirements on Data Protection from the Education Acts. ***For example:***

- Under **Section 9(g) of the Education Act, 1998**, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education

- Under **Section 20 of the Education (Welfare) Act, 2000**, the school must maintain a register of all students attending the school

- Under **section 20(5) of the Education (Welfare) Act, 2000**, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring. Headfort School will send copies of reports, to the Principal of the Post-Primary School in which the pupil has been enrolled. Where reports on pupils which have been completed by professionals, apart from Headfort School staff, are included in current pupil files, such reports are only passed to the Post-Primary school following express written permission having been sought and received from the parents of the said pupils.

- Under **Section 21 of the Education (Welfare) Act, 2000**, the school must record the attendance or non-attendance of students registered at the school on each school day

- Under **Section 28 of the Education (Welfare) Act, 2000**, the School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, Tusla, the National Education Welfare Board, or other centres of education) provided the School is satisfied that it will be used for a "relevant purpose" (which includes recording a person's educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training)

- The **Freedom of Information Act 1997** provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act these records could be disclosed if a request is made to that body

- Under **Section 26(4) of the Health Act, 1947** a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection

- Under **Children First Act 2015**, *mandated persons in* schools have responsibilities to report child welfare concerns to TUSLA- Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána)

Relationship to characteristic spirit of the school:

Headfort School seeks to:

- enable students to develop their full potential
- provide a safe and secure environment for learning
- promote respect for the diversity of values, beliefs, traditions, languages and ways of life in society

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, parents/guardians and others who interact with us. The school wishes to achieve these aims/missions while fully respecting individuals' rights to privacy and rights under the Data Protection legislation.

Personal Data

The *Personal Data* records held by the school **may** include:

Staff records:

a) **Categories of staff data:** As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:
   - Name, address and contact details, PPS number.
   - Name and contact details of next-of-kin in case of emergency.
   - Original records of application and appointment to promotion posts
   - Details of approved absences (career breaks, parental leave, study leave, etc.)
   - Details of work record (qualifications, classes taught, subjects, etc.)
   - Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
   - Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under Children First Act 2015

b) **Purposes:** Staff records are kept for the purposes of:
   - the management and administration of school business (now and in the future)
   - to facilitate the payment of staff, and calculate other benefits/ entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant)
   - to facilitate pension payments in the future
   - human resources management

- recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.
- to enable the school to comply with its obligations as an employer including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health and Welfare At Work Act. 2005)
- to enable the school to comply with requirements set down by the Revenue Commissioners, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies
- and for compliance with legislation relevant to the school.

c) Location and Security Procedures of Headfort School:

a. Manual records are kept in a secure, locked filing cabinet in a locked administration office only accessible to personnel who are authorised to use the data. Employees are required to maintain the confidentiality of any data to which they have access. Digital records are stored on a password-protected computer with adequate encryption and firewall software in a locked office. Bright HR, Call Soft and Sage systems are used to facilitate the payment and details of staff. Records of leave taken, illness, hours worked etc, is available through Bright HR.

Student records:

a) Categories of student data: These **may** include:

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school. These records may include:
  - name, address and contact details, PPS number,
  - date and place of birth,
  - names and addresses of parents/guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
  - religious belief
  - racial or ethnic origin
  - membership of the Traveller community, where relevant
  - whether they (or their parents) are medical card holders
  - whether English is the student's first language and/or whether the student requires English language support

- any relevant special conditions (e.g. special educational needs, health issues, etc.) which may apply

- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student
- Psychological, psychiatric and/or medical assessments
- Attendance records, class roll books / Aladdin System / Registers
- Photographs and recorded images of students (including at school events and noting achievements)
- Academic record – subjects studied, class assignments, examination results as recorded on official School reports
- Records of significant achievements
- Whether the student is exempt from studying Irish.
- Records of disciplinary issues/investigations and/or sanctions imposed
- Other records e.g. records of any serious injuries/accidents etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- Records of any reports the school (or its employees) have made in respect of the student to State departments and/or other agencies under Children First Act 2015.

b) Purposes: The purposes for keeping student records include:

- to enable each student to develop to their full potential
- to comply with legislative or administrative requirements
- to ensure that eligible students can benefit from the relevant additional teaching or financial supports
- to enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents of their child's educational progress or to inform parents of school events, etc.
- to meet the educational, social, physical and emotional requirements of the student
- photographs and recorded images of students are taken to celebrate school achievements, e.g. compile yearbooks, the school website, record school events, and to keep a record of the history of the school. Such records are taken and used in accordance with the '*Policy for the Safe Use of Photographs and Videos*'.
- to ensure that the student meets the school's admission criteria
- to ensure that students meet the minimum age requirement for attendance at Primary School.
- to ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities

- to furnish documentation/information about the student to, TUSLA, and other schools, etc. in compliance with law and directions issued by government departments
- to furnish, when requested by the student (or their parents/guardians in the case of a student under 18 years) documentation/information/references to second-level educational institutions.

c) **Location and Security:** The information on students is stored in two formats: both manual files containing hard copy of forms signed etc. and on computer files backed up and stored via Aladdin and Google system or on the office administration computer. Manual files are kept in a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Additional Information is also stored on the Aladdin data system. Teachers have access via Aladdin to their own class data only. Employees are required to maintain the confidentiality of any data to which they have access. Confidential reports, child protection report forms, Support documents are stored in limited access Google folders.

Parents' records

(a) Categories of data: the school may hold some or all of the following information about parents and/or guardians of pupils.

- Names, addresses and contact details (including any special arrangements with regard to guardianship, custody or access)
- Religious belief
- Racial or ethnic origin
- Occupation
- Financial circumstances if parents have requested and completed an Application Form for a Bursary
- Bank details in order to facilitate fee arrangements and for the return of any deposit

(b) Purposes: The provision of emergency contact details for students. To enable the School to manage the school's financial affairs, including and the issuing of fee invoices.

C Location: In a secure, locked filing cabinet and that only personnel who are authorised to use the data can access it and on the Accounts google account and Sage. Employees are required to maintain the confidentiality of any data to which they have access.

Prospective students and parents

(a) Categories of data: the school may hold some or all of the following information about prospective students and their parents and/or guardians:

- Names and addresses of prospective parents/legal guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
- Name, address and contact details, PPS Number, date and place of birth of prospective student
- Religious belief of prospective students and parents/guardians
- Racial or Ethnic Origin of prospective students and parents/guardians
- Occupation of prospective parents/legal guardians
- Information on prospective student's previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the prospective student
- Psychological, psychiatric and/or medical assessments of the prospective student
- Financial circumstances if prospective parents have requested and completed an Application Form.

(b) **Purposes:** To facilitate the application process for prospective students.

C Location: In a secure, locked filing cabinet and that only personnel who are authorised to use the data can access it and on the Admissions and Accounts google account. Employees are required to maintain the confidentiality of any data to which they have access.

Alumni (former students)

(a) Categories of data: the school may hold the following data in relation to former students of the school:

- name
- residential address
- email address

- telephone number
- correspondence

(b) **Purposes:** Alumni contact information is kept for the following purpose:

- To inform alumni of social gatherings and alumni events
- To share Newsletters to ensure alumni are kept up to date with the activities of the School eg for fundraising.

c) **Location.** On a secure google account of the Headmaster and stored with Mailchimp.. Employees are required to maintain the confidentiality of any data to which they have access.

Headfort Trust records:

a) Categories of Headfort Trust data: These **may** include:

- Name, address and contact details of each member of the Trust (including former members of the board of management)
- Records in relation to appointments to the Trust
- Minutes of Trust meetings and correspondence to the Trust which may include references to individuals.

b) Purposes: To enable the Headfort Trust to operate effectively.

c) Location: In a secure, locked filing cabinet and that only personnel who are authorised to use the data can access it and on the Headmasters google account and laptop. Employees are required to maintain the confidentiality of any data to which they have access.

d) **Security:** Minutes from Board Meetings are emailed in advance of a meeting to Board members and not to be shared with any one else.

Other information that may be retained by the school includes:

For Example:

The school will hold other records relating to individuals. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database). Some examples of the type of other records which the school will hold are set out below (this list is not exhaustive):

Creditors

(a) **Categories of data:** the school may hold some or all of the following information about creditors (some of whom are self-employed individuals):

- Name, address, contact details, PPS number
- Tax details, bank details and amount paid.

(b) **Purposes:** This information is required for routine management and administration of the school's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

(c) **Location / Security:** In a secure, locked office and on Sage that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. We use on-line banking in the school where possible so much of this detail is stored on this system. This is regulated by Bank of Ireland online banking regulations.

Charity Tax-back Forms

(a) **Categories of data:** The school may hold the following data in relation to donors who have made charitable donations to the school:

- Name, address, telephone number, PPS number
- Tax rate, signature and the gross amount of the donation.

(b) **Purposes:** Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate certificate is the parents name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the School in the case of audit by the Revenue Commissioners.

(c) **Location/Security:** In a secure, filing cabinet and on Accounts computer/ Google account that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Assessment results

(a) **Categories:** The school will hold data comprising examination results in respect of its students. These include class, mid-term, annual, continuous assessment and standardised test results.

(b) **Purposes:** The main purpose for which these examination results and other records are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardians about their education. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables.

(c) **Location / Security:** Assessments are stored in either or both of the following: manual files containing a hard copy of assessments and on computer files backed up or stored via the Aladdin system. Employees are required to maintain the confidentiality of any data to which they have access. Assessment information kept on computers via Aladdin is generally aggregated results. The computer and Aladdin are password protected. Any assessment information on individual children is kept locked on the pupil's individual file. This also applies to reports by any outside agency or professional about an individual pupil, only personnel who are authorised to use the data can access this.

Garda Vetting Information

All adults working with children in any capacity within the school must be Garda vetted. Completed vetting forms are sent to the Garda and the results of vetting process are stored manually in a locked filing cabinet in the office to which only authorised personnel may have access.

Links to other policies and to curriculum delivery

Our school policies need to be consistent with one another, within the framework of the overall School Plan. Relevant school policies already in place or being developed or reviewed, shall be examined with reference to the data protection policy and any implications which it has for them shall be addressed.

The following policies may be among those considered:

- Child Protection Policy
- Anti-Bullying Policy

- Code of Behaviour, including Mobile Phone Code
- Admissions Policy
- ICT Acceptable Usage Policy
- SPHE etc.

Processing in line with data subject's rights

Data in this school will be processed in line with the data subjects' rights. Data subjects have a right to:

- Know what personal data the school is keeping on them
- Request access to *any data* held about them by a data controller
- Prevent the processing of their data for direct-marketing purposes
- Ask to have inaccurate data amended
- Ask to have data erased once it is no longer necessary or irrelevant.

Data Processors

Where the school outsources to a data processor off-site, it is required by law to have a written contract in place (Written Third party service agreement). Headfort School's third party agreement specifies the conditions under which the data may be processed, the security conditions attaching to the processing of the data and that the data must be deleted or returned upon completion or termination of the contract.

Personal Data Breaches

All incidents in which personal data has been put at risk must be reported to the Office of the Data Protection Commissioner within 72 hours

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Trust must communicate the personal data breach to the data subject without undue delay. If a data processor becomes aware of a personal data breach, it must bring this to the attention of the data controller (Trust) without undue delay.

Dealing with a data access requests

Individuals are entitled to a copy of their personal data on written request

The individual is entitled to a copy of their personal data

Request must be responded to within one month. An extension may be required e.g. over holiday periods

No fee usually required - You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances. No personal data can be supplied relating to another individual apart from the data subject.

What we may need from you - We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond - We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Providing information over the phone

In our school, any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the school over the phone. In particular the employee should:

- Check the identity of the caller to ensure that information is only given to a person who is entitled to that information
- Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified
- Refer the request to the principal for assistance in difficult situations. No employee should feel forced into disclosing personal information.

Implementation arrangements, roles and responsibilities

In our school the Headfort Trust is the data controller and the Headmaster will be assigned the role of coordinating the implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities.

The following personnel have responsibility for implementing the Data Protection Policy:

Name	Responsibility
Headfort Trust	Data Controller
Headmaster	Implementation of Policy
Teaching Personnel	Awareness of responsibilities, security measures, storage and confidentiality issues as outlines in this policy

Administrative personnel:	Awareness of responsibilities, security measures, storage and confidentiality issues as outlines in this policy

Ratification & communication

When the Data Protection Policy has been ratified by the Headfort trust, it becomes the school's agreed Data Protection Policy. It should then be dated and circulated within the school community. The entire staff must be familiar with the Data Protection Policy and ready to put it into practice in accordance with the specified implementation arrangements. It is important that all concerned are made aware of any changes implied in recording information on students, staff and others in the school community. Parents/guardians and students should be informed of the Data Protection Policy from the time of enrolment of the student e.g. by including the Data Protection Policy as part of the Enrolment Pack, by either enclosing it or incorporating it as an appendix to the enrolment form.

Monitoring the implementation of the policy

The implementation of the policy shall be monitored by the principal and the board of management.

At least one annual report should be issued to the board of management to confirm that the actions/measures set down under the policy are being implemented.

Reviewing and evaluating the policy

The policy will be reviewed and evaluated regularly. On-going review and evaluation will take cognizance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills or TUSLA), legislation and feedback from parents/guardians, students, school staff and others. The policy will be revised as necessary in the light of such review and evaluation and within the framework of school planning

Signed: _____

Chairperson Headfort Trust

Date: 27th November 2024

P McCormick
27/11/24

Appendix 1

Data Retention Periods for schools

Pupil Related	Retention Periods
School Register/Roll Books	Indefinitely
Enrolment Forms	Hold until Pupil is 25 Years
Disciplinary notes	Never Destroy
Test Results – Standardised	Hold until pupil is 25 Years
Psychological Assessments etc.	Never Destroy
SEN Files/IEPS	Never Destroy
Accident Reports	Never Destroy
Child Protection Reports/Records	Never Destroy
Interview Records	
Interview Board Marking Scheme Interview notes (for unsuccessful candidates)	18 months from close of competition plus 6 months in case Equality Tribunal needs to inform school that a claim is being taken
Staff Records	
Contract of Employment Vetting Records Disciplinary notes Sickness Accident/Injury at work Reports	Retention for duration of employment + 7 years (6 years to make a claim against the school plus 1 year for proceedings to be served on school)
BoM Records	
Trust Agenda and Minutes	Indefinitely
CC TV Recordings	28 days normally. In the event of criminal investigation – as long as is necessary
Payroll & Taxation	Revenue require a 6-year period after the end of the tax year
Invoices/receipts	Retain for 7 Years
Audited Accounts	Indefinitely

Why, in certain circumstances, does the Data Protection Commission recommend the holding of records until the former pupil has attained 25 years of age?

The reasoning is that a pupil reaches the age of majority at 18 years and that there should be a 6-year limitation period in which it would be possible to take a claim against a school, plus 1 year for proceedings to be served on a school. The Statute of Limitations imposes a limit on a right of action so that after a prescribed period any action can be time barred.

Appendix 2

Use of the Aladdin system -

One of the IT service companies that we use includes Cloudware Limited (T/A Aladdin Schools) ("Aladdin"). Aladdin processes personal data on behalf of the school in order to provide an online management information system.
The schools liaison person for any queries relevant to use of the Aladdin system is the Headmaster.

Anyone provided with a username and password and who is authorised to use the Aladdin system by the school should adhere to and be aware of the following:

- users may be allocated different access rights to the Aladdin system. The access rights are solely determined by the school. If you have any concern over the access rights that you have please contact the Aladdin school liaison;
- a log is taken of some actions undertaken by the user when using the Aladdin system and made available to the school;
- a unique username and password is provided to each user. Users should keep their username and password confidential and not disclose it to anybody or allow any person to access the system using their username and password;
- the Aladdin system should only be used for the purposes of managing internal school administration activities and for no other purpose. The Aladdin system should not be accessed in the event of suspension or termination of the users position at the school. The school is responsible for ensuring that access to the Aladdin system for terminated or suspended users is disabled;
- each user should ensure they are familiar with the Aladdin system before use. All queries should be referred to the Aladdin liaison person mentioned above;
- the user should notify the Aladdin liaison person in the event of any misuse or loss of their username and password
- the user should only login to the Aladdin system when in a secure and non-public environment, e.g. the school or home of the user;
- the user should sign out of the Aladdin system or lock their device when leaving the device unattended;
- the Aladdin system should not be used to deal with emergency situations and it should not be relied upon during such times;

Headfort School
Kells
Co. Meath
A82 H7P2
+353 (0)46-9271116

- users are responsible for ensuring that all communications sent to parents or guardians using the Aladdin system are accurate and are sent to parents/guardians for whom the school has appropriate and up to date consent and contact details;
- the Aladdin system should not be accessed through an unsecure network or internet connection. If in doubt, the user should wait until in a secure environment before accessing the Aladdin system.
- information available through the Aladdin system should only be printed or saved to an electronic device where absolutely necessary. Any hardcopy or electronic files originating from the Aladdin system should be treated in accordance with the relevant provisions of this policy; and
- users may be able to access the websites of other third-party service providers when accessing the Aladdin system. When the user accesses a third-party website from the Aladdin system they are leaving the Aladdin system and appropriate due diligence should be undertaken before sharing any personal data with that third party. The Aladdin liaison person should be contacted if the user is in any doubt.

For further information about Aladdin please go to: https://www.aladdin.ie/