Heywood Community School

Data Protection Policies

Data Protection Policy

CCTV Policy

Records Retention Schedule

Data Access Procedures Policy

Data Request Form

Personal Data Security Breach Code of Practice

Data Protection Policies

Data Protection Policy of Heywood Community School

The school's Data Protection Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988 and 2003.

The policy applies to all school staff, the Board of Management, 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 sensitive personal data will be protected by the school.

Data Protection Principles

The school 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 school is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 and 2003 which can be summarised as follows:

- **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.
- **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.
- **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.
- **Keep Personal Data safe and secure:** Only those with a genuine reason for doing so may gain access to the information. Sensitive Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the school premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

- **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.
- **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.
- **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 comply with DES guidelines on the storage of Personal Data and Sensitive Personal Data relating to a student. In the case of members of staff, the school will comply with both 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**.**
- **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.

Scope

Purpose of the Policy: The Data Protection Acts 1988 and 2003 apply to the keeping and processing of Personal Data, both in manual and electronic form. 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 board of management, 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 school staff:
Data means information in a form that can be processed. It includes both automated data (e.g. electronic data) and manual data. *Automated data* means any information on computer, or information recorded with the intention that it be processed by computer.

Manual data means information that is kept/recorded as part of a relevant filing system or with the intention that it form part of *a relevant filing system.*

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily, quickly and easily accessible.

Personal Data means data relating to 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.

Sensitive Personal Data refers to Personal Data regarding a person's

- racial or ethnic origin, political opinions or religious or philosophical beliefs
- membership of a trade union
- physical or mental health or condition or sexual life
- commission or alleged commission of any offence or
- any proceedings for an offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings, criminal convictions or the alleged commission of an offence.

Data Controller for the purpose of this policy is the Board of Management of Heywood Community School.

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 and 2003. 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. As more and more data is generated electronically and as technological advances enable the easy distribution and retention of this data, the challenge of meeting the school's legal responsibilities has increased.

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 principal and board of management 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 Board of Management.

Other Legal Obligations:

Implementation of this policy takes into account the school's other legal obligations and responsibilities.

- 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
- 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, the National Education Welfare Board, the National Council for Special Education, other schools, 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)
- Under **Section 14 of the Education for Persons with Special Educational Needs Act, 2004**, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers ("SENOs") such information as the Council may from time to time reasonably request
- 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 (such as the Department of Education and Skills, etc.) 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: National Guidance for the Protection and Welfare of Children (2011)** published by the Department of Children & Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect 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 (School's mission/vision/aims)

Heywood Community School seeks to:

- enable each student 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 Acts.

Personal Data

The Personal Data records held by the school may include:

A. 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
- 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 mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures).

(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 Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies
- for compliance with legislation relevant to the school.

(c) Location:

Manual staff records will be stored in a secure locked press in a secure locked room 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. Nonsensitive computerised staff records will be stored on the school's computer system with password protection

(d) Security: Staff records will be kept in manual format (personal file within a relevant filing system) in a locked press in a locked room, or in password protected computerised format (non-sensitive data).

B. 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
- Photographs and recorded images of students (including at school events and noting achievements). See the template "Guidance on Taking and Using Images of Children in Schools"
- Academic record – subjects studied, class assignments, examination results as recorded on official school reports.
- Records of significant achievements
- Whether the student is repeating the Leaving Certificate
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Garda vetting outcome record (where the student is engaged in work experience organised with or through the school/ETB which requires that they be Garda vetted)
- 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 mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).

(b) Purposes:

The purposes for keeping student records are:

- 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 support the provision of religious instruction
- 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, compile yearbooks, establish a 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 school's "Guidance for Taking and Using Images of Pupils in Schools"
- to ensure that the student meets the school's admission criteria
- to ensure that students meet the minimum age requirements for their course,
- 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 the Department of Education and Skills, the National Council for Special Education, 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 third-level educational institutions and/or prospective employers
- In respect of a work experience placement, (where that work experience role requires that the student be Garda vetted) the School will assist the student in obtaining their Garda vetting outcome (with the consent of the student and their parent/guardian) in order to furnish a copy of same (with the consent of the student and the student's parent/guardian) to the work experience employer.

(c) Location: Manual student records will be stored in a secure locked press in a secure locked room that only personnel who are authorised to use the data can access. Computerised student records will be stored on the school's computer system with password protection. Employees are required to maintain the confidentiality of any data to which they have access.

(d) Security: Student records will be kept in manual format (personal file within a relevant filing system, in group files sorted by category) in a locked press in a locked room, or in password protected computerised format.

C. Board of management records:

(a) Categories of board of management data: These may include:

- Name, address and contact details of each member of the board of management (including former members 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.

(**b) Purposes**: To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of board appointments and decisions.

(c) Location: Board of Management records will be stored in a secure locked press in a secure locked room that only personnel who are authorised to use the data can access. Computerised Board of Management records will be stored on the school's computer system with password protection. Employees are required to maintain the confidentiality of any data to which they have access.

(e) Security: Board of Management records will be kept in manual format (files within a relevant filing system) in a locked press in a locked room, or in password protected computerised format.

D. Other records:

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
- 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: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Computerised records of creditors will be stored on the school's computer system with password protection. Employees are required to maintain the confidentiality of any data to which they have access.

(d) Security: Creditors' records will be kept in manual format (files within a relevant filing system) in a locked press in a locked room, or in password protected computerised format.

CCTV images/recordings

(a) Categories: CCTV is installed externally and internally as detailed in the CCTV Policy. The CCTV systems may record images of staff, students and members of the public who visit the premises.

(b) Purposes: Safety and security of staff, students and visitors and to safeguard school property and equipment.

(c) Location: Cameras are located externally and internally as detailed in the CCTV Policy. Recording equipment is located in the reception office of school.

(d) Security: Access to images/recordings is restricted to the Principal & Deputy Principal of Heywood Community School. Hard disk recordings are retained for 28 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988 and 2003.

Examination 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 mock- examinations 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 subject choices and levels. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.

(c) Location: In a secure, locked filing cabinet 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.

(d) Security: Examination results will be kept in manual format (personal file within a relevant filing system, in group files sorted by category) in a locked press in a locked room, or in password protected computerised format.

October Returns

(**a) Categories**: At the beginning of each academic year (and for 1st year or transferring students, on enrolment) parents/guardians and students are asked to provide the school with certain information so that the School can make returns to the Department of Education and Skills ("DES") referred to as "October Returns". These October Returns will include sensitive personal data regarding personal circumstances which are provided by parents/guardians and students on the basis of explicit and informed consent. The October Return contains individualised data (such as an individual student's PPS number) which acts as an "identifier" for the DES to validate the data that belongs to a recognised student. The DES also transfers some of this data to other government departments and other State bodies to comply with legislation, such as transfers to the Department of Social Protection pursuant to the Social Welfare Acts, transfers to the State Examinations Commission, transfers to the Educational Research Centre, and transfers to the Central Statistics Office pursuant to the Statistics Acts. The data will also be used by the DES for statistical, policy-making and

research purposes. However the DES advises that it does not use individual data, but rather aggregated data is grouped together for these purposes. The DES has a data protection policy which can be viewed on its website (www.education.ie). The DES has also published a "Fair Processing Notice" to explain how the personal data of students and contained in October Returns is processed. This can also be found on www.education.ie (search for Circular Letter 0047/2010 in the "Circulars" section).

(b) Purposes: The school asks parents/guardians and students to complete October Returns for the purposes of complying with DES requirements to determine staffing and resource allocations and to facilitate the orderly running of the school. The main purpose of the October Returns is for the DES to determine whether the student qualifies for English language support and/or additional resources and support to meet their particular educational needs. The October Returns are submitted to the DES electronically. The DES has their own policy governing the security of the data sent to them by all post-primary schools. The co-operation of each student and/or their parents/guardians in completing the October Return is greatly appreciated as the school's aim is to ensure that each student is assisted in every way to ensure that s/he meets his/her full potential.

(c) Location: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Computerised records of October Returns will be stored on the school's computer system and on the DES online facility with password protection. Employees are required to maintain the confidentiality of any data to which they have access.

(d) Security: Details for October Returns in manual format (files within a relevant filing system) in a locked press in a locked room, or in password protected computerised format will be stored on the school's computer system and on the DES online facility with password protection

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.

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:

(a) Request access to any data held about them by a data controller

(b) Prevent the processing of their data for direct-marketing purposes

(c) Ask to have inaccurate data amended

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Dealing with a data access request

Under **Section 3 of the Data Protection Acts,** an individual has the right to be informed whether the school holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request in writing and the data controller will accede to the request within 21 days.

The right under Section 3 must be distinguished from the much broader right contained in Section 4, where individuals are entitled to a copy of their data.

Section 4 access request

- Individuals are entitled to a copy of their personal data on written request.
- The individual is entitled to a copy of their personal data (subject to some exemptions and prohibitions set down in Section 5 of the Data Protection Act)
- Request must be responded to **within 40 days**
- Fee may apply but cannot exceed **€6.35**
- Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the school as data controller to comply with the second request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on a case-by-case basis.
- No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant.
- Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the school refuse to furnish the data to the applicant.

Providing information over the phone

In our school, secretaries 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 Board of Management is the data controller and the Principal will be assigned the role of co-ordinating 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
Board of Management:	Data Controller
Principal:	Implementation of Policy
Teaching personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

Ratification & Communication

When the Data Protection Policy has been ratified by the Board of Management, 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 Principal will ensure that all policies are brought to the attention of Year heads, Coordinators, Teachers, Secretarial and Caretaking staff. It is then the duty of each individual within the School Community to read these policies closely and ensure that they are familiar with the policies and can comply with the same.

The principal will be responsible for maintaining and updating student records. The principal may delegate these duties to other appropriate members of staff. Other school personnel may update student records with the approval and sanction of the Principal.

The policy will be revised as necessary taking cognisance of changing information or guidelines(e.g. from the Data Protection Commissioner, Departmnt of Education and Skills or Solas), legistlation and feedback from parents/guardians and school staff.

This Policy was adopted by the Board of Management of Heywood Community School on _____ (date).

Signed:_____ (Chairperson of Board of Management)

Date:_____

Signed: _____(Principal)

Date:_____

CCTV Policy

Heywood Community School

INTRODUCTION

Closed Circuit Television Systems (CCTVS) are installed in Heywood Community School. Their operation will be reviewed regularly in consultation with staff, the board of management and the parents association.

1. PURPOSE OF POLICY

"The purpose of this policy is to regulate the use of Closed Circuit Television and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of Heywood Community School"

CCTV systems are installed (both internally and externally) in premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day. CCTV surveillance at the school is intended for the purposes of:

- protecting the school buildings and school assets, both during and after school hours
- promoting the health and safety of staff, pupils and visitors
- preventing bullying
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism)
- supporting the Gardai in a bid to deter and detect crime
- assisting in identifying, apprehending and prosecuting offenders
- ensuring that the school rules are respected so that the school can be properly managed

2. SCOPE

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material.

3. GENERAL PRINCIPLES

Heywood Community School as the corporate body has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, students and invitees to its premises. Heywood Community School owes a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the school community by integrating the best practices governing the public and private surveillance of its premises.

The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is

prohibited by this policy e.g. CCTV will not be used for monitoring employee **performance.**

Information obtained through the CCTV system may only be released when authorised by the Principal, following consultation with the Chairperson of the Board of Management. Any requests for CCTV recordings/images from An Garda Síochána will be fully recorded and legal advice will be sought if any such request is made. (See "Access" below). If a law enforcement authority, such as An Garda Síochána, is seeking a recording for a specific investigation, An Garda Síochána may require a warrant and accordingly any such request made by An Garda Síochána should be requested in writing and the school/ETB will immediately seek legal advice.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the school/ETB, including Equality & Diversity Policy, Dignity at Work Policy, Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, including the provisions set down in equality and other educational and related legislation.

This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

Video monitoring of public areas for security purposes within school's premises is limited to uses that do not violate the individual's reasonable expectation to privacy.

Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the school or a student attending the school.

All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by the Board of Management of Heywood Community School. Recognisable images captured by CCTV systems are "personal data." They are therefore subject to the provisions of the Data Protection Acts 1988 and 2003.

4. JUSTIFICATION FOR USE OF CCTV

Section 2(1)(c)(iii) of the Data Protection Acts requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that Heywood Community School needs to be able to justify the obtaining and use of personal data by means of a CCTV system. The use of CCTV to control the perimeter of the school buildings for security purposes has been deemed to be justified by the Board of Management. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

CCTV systems will not be used to monitor normal teacher/student classroom activity in school.

In other areas of the school where CCTV has been installed, e.g. hallways, stairwells, locker areas, the Principal has demonstrated that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues that have arisen prior to the installation of the system.

5. LOCATION OF CAMERAS

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. Heywood Community School has endeavoured to select locations for the installation of CCTCV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV Video Monitoring and Recording of Public Areas in Heywood Community School may include the following:

- **Protection of school buildings and property:** The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services
- **Monitoring of Access Control Systems:** Monitor and record restricted access areas at entrances to buildings and other areas
- **Verification of Security Alarms:** Intrusion alarms, exit door controls, external alarms
- **Video Patrol of Public Areas:** Parking areas, Main entrance/exit gates, Traffic Control
- **Criminal Investigations (carried out by An Garda Síochána):** Robbery, burglary and theft surveillance

6. COVERT SURVEILLANCE

Heywood Community School will not engage in covert surveillance.

Where An Garda Síochána requests to carry out covert surveillance on school premises, such covert surveillance may require the consent of a judge. Accordingly, any such request made by An Garda Síochána will be requested in writing and the school will seek legal advice.

7. NOTIFICATION – SIGNAGE

The Principal will provide a copy of this CCTV Policy on request to staff, students, parents and visitors to the school. This policy describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use. The location of CCTV cameras will also be indicated to the Board of Management. Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to Heywood Community School property. Signage shall include

the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

WARNING CCTV cameras in operation Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behaviour, the prevention of bullying, for the safety of our staff and students and for the protection of Heywood Community School and its property. This system will be in operation 24 hours a day, every day. These images may be passed to An Garda Síochána. This scheme is controlled by Heywood Community School For more information contact 05787 33333

Appropriate locations for signage will include:

- at entrances to premises i.e. external doors, school gates
- reception area
- at or close to each internal camera

8. STORAGE & RETENTION

Section 2(1)(c)(iv) of the Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. A data controller needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a month (28 days), except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue. Accordingly, the images captured by the CCTV system will be retained for a maximum of 28 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue. The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Principal. The Principal may delegate the administration of the CCTV System to another staff member. In certain

circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above (such individuals may include the Gardai, the Deputy Principal, the relevant Year Head, other members of the teaching staff, representatives of the Department of Education and Skills, representatives of the HSE and/or the parent of a recorded student). When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

9. ACCESS

Access to the CCTV system and stored images will be restricted to authorised personnel only i.e. Principal of school or a person delegated by the Principal. In relevant circumstances, CCTV footage may be accessed in any of the following cases:

- By An Garda Síochána where Heywood community School (or its agents) are required by law to make a report regarding the commission of a suspected crime
- Following a request by An Garda Síochána when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on Heywood Community School property
- To the HSE and/or any other statutory body charged with child safeguarding
- To assist the Principal in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed
- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to Heywood Community School
- To individuals (or their legal representatives) subject to a court order.
- To the State claims Agency in order to pursue a claim for damage done to the insured property.

Requests by An Garda Síochána: Information obtained through video monitoring will only be released when authorised by the Principal following consultation with the Chairperson of the Board of Management. If An Garda Síochána request CCTV images for a specific investigation, An Garda Síochána may require a warrant and accordingly any such request made by An Garda Síochána should be made in writing and the school should immediately seek legal advice.

Access requests: On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. To exercise their right of access, a data subject must make an application in writing to the school

Principal. The school may charge up to €6.35 for responding to such a request and must respond **within 40 days.**

Access requests can be made to the following: Mr. Philip Bowe, Heywood Community School, Ballinakill, Co. Laois.

A person should provide all the necessary information to assist Heywood Community School in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the school.

In giving a person a copy of their data, the school may provide a still/series of still pictures, a tape or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

10. **RESPONSIBILITIES**

The Principal will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by Heywood Community School
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within Heywood Community School
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring at Heywood Community School is consistent with the highest standards and protections
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- Maintain a record of access (e.g. an access log) to or the release of any material recorded or stored in the system
- Ensure that monitoring data is not duplicated for release
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- Provide a list of the CCTV cameras and the associated monitoring equipment and the capabilities of such equipment, located in Heywood Community School to the Board of Management for formal approval
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. NOTE: [Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by An Garda Síochána].
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment

- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place
- Co-operate with the Health & Safety Officer of Heywood Community School in reporting on the CCTV system in operation in the school
- Advise the Board of Management that adequate signage at appropriate and prominent locations is displayed as detailed above
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 28 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Chairperson of the Board.
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas
- Ensure that where An Garda Síochána request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of the Chairperson of the Board.

11. IMPLEMENTATION & REVIEW

The policy will be reviewed and evaluated from time to time. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, An Garda Síochána, Department of Education and Skills, Audit units (internal and external to the school), the national management bodies, legislation and feedback from parents/guardians, students, staff and others.

The date from which the policy will apply is the date of adoption by the Board of Management. Implementation of the policy will be monitored by the Principal of the school.

APPENDIX 1 - DEFINITIONS

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy;

CCTV – Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.

The Data Protection Acts – The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All school/ETB staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Personal Data – Data relating to 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.

Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and/or section 4 of the Data Protection Acts.

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 Subject – an individual who is the subject of personal data.

Data Controller - a person who (either alone or with others) controls the contents and use of personal 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 Acts place responsibilities on such entities in relation to their processing of the data.

Records Retention Schedule

Heywood Community School

Retention of Records

Schools and ETBs as *data controllers* must be clear about the length of time for which personal data will be kept and the reasons why the information is being retained. In determining appropriate retention periods, regard must be had for any statutory obligations imposed on a data controller. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner. It may also be anonymised to remove any personal data. Anonymisation must be irrevocable; removing names and addresses may not necessarily be sufficient.

In order to comply with this legal requirement, Heywood Community School has assigned specific responsibility and introduced procedures for ensuring that files are purged regularly and securely and that personal data is not retained any longer than is necessary. All records will be periodically reviewed in light of experience and any legal or other relevant indications (**See Appendix 2).**

IMPORTANT: In all cases, schools should be aware that where proceedings have been initiated, are in progress, or are reasonably foreseeable (although have not yet been taken against the school/board of management/an officer or employee of the school (which may include a volunteer)), all records relating to the individuals and incidents concerned should be preserved and should under no circumstances be deleted, destroyed or purged. The records may be of great assistance to the school in defending claims made in later years.

WARNING: In general, the limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim and the Statue of Limitations may be different in every case. In all cases where reference is made to "18 years" being the date upon which the relevant period set out in the Statute of Limitations commences for the purposes of litigation, the school must be aware that in some situations (such as the case of a student with special educational needs, or where the claim relates to child sexual abuse, or where the student has not become aware of the damage which they have suffered, and in some other circumstances), the Statute of Limitations may not begin to run when the student reaches 18 years of age and specific legal advice should be sought by schools on a case-by-case basis. In all cases where retention periods have been recommended with reference to the relevant statutory period in which an individual can make a claim, these timeframes may not apply where there has been misrepresentation, deception or fraud on the part of the respondent/defendant. In such a circumstance, the school/ETB should be aware that the claim could arise many years after the incident complained of and the courts/tribunals/employment fora may not consider the complainant to be "out of time" to make their claim.

Data Access Procedures Policy
Heywood Community School

The Data Protection Acts, 1988 and 2003 provide for a right of access by an individual data subject to personal information held at Heywood Community School. The following procedure is provided to ensure compliance with the school's obligations under the Acts and governs the manner in which requests for access to personal data will be managed by Heywood Community School. A data subject would be required to familiarize themselves with the procedure and to complete the **Data Access Request Form** which will assist the school in processing the access request where personal information (or in the case of a parent/guardian making an access request on behalf of a student, personal information in relation to their child) as a data subject is processed and retained by Heywood Community School. It is important to note that only personal information relating to the individual (or in the case of a parent/guardian making an access request on behalf of a student, only personal information in relation to his/her/their child) will be supplied. No information will be supplied that relates to another individual.

Important note to students making access requests

Where a student (aged under 18 years) makes an access request, the school may inform the student that:

(a) Where they make an access request, their parents will be informed that they have done so and
(b) A complete copy of the access request materials being furnished to the data subject by the school will also be furnished to the student's parent/guardian.

This is provided for in the school's Data Protection Policy. The right of access under the Data Protection Acts is the right of the data subject. However, there may be some data held by the school which may be of a sensitive nature and the school will have regard to the following guidance issued by the Office of the Data Protection Commissioner in relation to releasing such data:

- A student aged **eighteen years or older** (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves.

- If a student aged **eighteen years or older** has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student.

- A student aged from **twelve up to and including seventeen** can be given access to their personal data, depending on the age of the student and the nature of the record, i.e. it is suggested that:

- If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access
- If the information is of a sensitive nature, it would be prudent to seek parental/guardian consent before releasing the data to the student
- If the information would be likely to be harmful to the individual concerned, parental/guardian consent should be sought before releasing the data to the student.

- In the case of students **under the age of twelve,** an access request may be made by their parent or guardian on the student's behalf. However, the school must note that the right of access is a right of the data subject themselves (i.e. it is the right of the student). Therefore, access documentation should be addressed to the child at his/her address which is registered with the school as being his/her home address. **It should not be addressed or sent to the parent who made the request.** For further information, see "Important Note to Parents Making Access Requests on Behalf of their Child" below.

Important note to parents making access requests on behalf of their child

Where a parent/guardian makes an access request on behalf of their child (a student aged under 18 years), the right of access is a right of the data subject (i.e. it is the student's right). In such a case, the access materials will be sent to the child, not to the parent who requested them. This means that the access request documentation will be sent to the address at which the child is registered on the school's records and will be addressed to the child. The documentation will not be sent to or addressed to the parent/guardian who made the request. Where a parent/guardian is unhappy with this arrangement, the parent/guardian is invited to make an application to court under section 11 of the Guardianship of Infants Act 1964. This provision enables the court (on application by a guardian) to make a direction on any question affecting the welfare of the child. Where a court issues an order stating that a school should make certain information available to a parent/guardian, a copy of the order should be given to the school by the parent/guardian and the school can release the data on foot of the court order.

Individuals making an access request

On making an access request, any individual (subject to the restrictions in Notes A and B below) about whom a school keeps *Personal Data*, is entitled to:

- a copy of the data which is kept about him/her (unless one of the exemptions or prohibitions under the Data Protection Acts apply, in which case the individual will be notified of this and informed of their right to make a complaint to the Data Protection Commissioner)
- know the purpose/s for processing his/her data
- know the identity (or the categories) of those to whom the data is disclosed know the source of the data, unless it is contrary to public interest

Data access requirements

To make an access request, you as a data subject must:

- Apply in writing requesting access to your data under section 4 Data Protection Acts or, alternatively, request an Access Request Form which will greatly assist the school in processing your access request more quickly.

Correspondence should be addressed to the Principal or the Chairperson of the Board of Management

You will be provided with a form which will assist the school in locating all relevant information that is held subject to the exceptions and prohibitions outlined in **Appendix A.** The school **reserves the right to request official proof of identity (**e.g. photographic identification such as a passport or driver's licence) where there is any doubt on the issue of identification**.**

- On receipt of the access request form, a co-ordinator will be appointed to check the validity of your access request and to check that sufficient information to locate the data requested has been supplied (particularly if CCTV footage/images are to be searched).

The co-ordinator is either the Principal or the Chairperson of the Board.

It may be necessary for the co-ordinator to contact you in the event that further details are required with a view to processing your access request.

- The co-ordinator will log the date of receipt of the valid request and keep a note of all steps taken to locate and collate the requested data.
- The co-ordinator will ensure that all relevant manual files (held within a "relevant filing system") and computers are checked for the data in respect of which the access request is made.
- The co-ordinator will ensure that the information is supplied promptly and within the advised timeframes in items 7, 8 and 9 as appropriate.
- **Where a request is made under Section 3 of the Data Protection Acts**, the following information will be supplied: (i) what the school holds by way of personal information about you ((or in the case of a request under section 3 made by a parent/guardian of a student aged under 18 years, then the personal information held about that student) and (ii) a description of the data together with details of the purposes for which his/her data is being kept will be provided. Actual copies of your personal files (or the personal files relating to the student) will not be supplied. No personal data can be supplied relating to another individual. A response to your request will be provided within 21 days of receipt of the access request form and no fee will apply.
- **Where a request is made under Section 4 of the Data Protection Acts**, the following information will be supplied within **40 days and an administration fee of €6.35 will apply**. The individual is entitled to:

- A copy of the data which is kept about him/her (unless one of the exemptions or prohibitions under the Data Protection Acts applies, in which case the individual will be notified of this and informed of their right to make a complaint to the Data Protection Commissioner)
- Be advised of the purpose/s for processing his/her data
- Be advised of the identity (or the categories) of those to whom the data is disclosed
- Be advised of the source of the data, unless it is contrary to public interest

- Where a request is made with respect **to examination results** an increased time limit of **60 days** from the date of the first publication of the results or from the date of the access request, whichever is the later will apply.

- Before supplying the information requested to you as data subject (or where the access request is made on behalf of a student aged under 18 years, information relating to the student), the co-ordinator will check each item of data.

- **Where a school may be unsure as to what information to disclose, the school reserves the right to seek legal advice**

- The co-ordinator will ensure that the information is provided in an intelligible form (e.g. codes explained) or will provide an explanation.
- Number the documents supplied.
- Have the response "signed-off" by an appropriate person. - In the case of C&C schools, this function is undertaken by either the Principal or the Chairperson of the Board
- The school will respond to your access request within the advised timeframes contingent on the type of request made.
- The school reserves the right to supply personal information to an individual in an electronic format e.g. on tape, USB, CD etc.
- Where a subsequent or similar access request is made after the first request has been complied with, the school has discretion as to what constitutes a reasonable interval between access requests and this will be assessed on a case-by case basis.
- Where you as an individual data subject may seek to rectify incorrect information maintained by the school, please notify the school and a form will be supplied to you for this purpose. You should however note that the right to rectify or delete personal data is not absolute. You have the right to make a complaint to the Data Protection Commissioner about a refusal. Where the school declines to rectify or delete the personal data as you have instructed, the school may propose to supplement your personal record, pursuant to section 6(1)(b) Data Protection Acts.
- In circumstances where your access request is refused, Heywood Community School will write to you explaining the reasons for the refusal and the administration fee, if provided, will be returned. In such circumstances, you have the right to make a complaint to the Office of the Data Protection Commissioner www.dataprotection.ie. Similarly, the administration access fee will be refunded to you if the school has to rectify, supplement or erase your personal data.

- **Where requests are made for CCTV footage,** an application must be made in writing and the timeframe for response is within 40 days. All necessary information such as the date, time and location of the recording should be given to the school to assist the school in dealing with your request. Where the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data. In providing a copy of personal data, the school may provide the materials in the form of a still/series of still pictures, a tape, disk, USB, with relevant images. Other people's images will be obscured before the data is released. If other people's images cannot be obscured, then the images/recordings may not be released.

There are a number of exceptions to the general rule of right of access, including those specified in Notes A and B in **Appendix A. This procedure is regularly reviewed in line with the school's commitment to its responsibilities under data protection**.

Appendix A Note A: Access requests by students

- A student aged **eighteen years or older** (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves.
- If a student aged **eighteen years or older** has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student.
- A student aged from **twelve up to and including seventeen** can be given access to their personal data, depending on the age of the student and the nature of the record, i.e. it is suggested that
- If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access
- If the information is of a sensitive nature, it would be prudent to seek parental/guardian consent in writing before releasing the data to the student. Where the parent/guardian does not give their consent to releasing the data to the student, legal advice should be sought
- If the information would be likely to be harmful to the individual concerned, parental/guardian consent should be sought before releasing the data to the student.
- In the case of students **under the age of twelve**, an access request may be made by their parent or guardian on the student's behalf. The consent of the child need not be obtained. However, the school/ETB must note that the right of access is a right of the data subject themselves (i.e. it is the right of the student). Therefore, access documentation should be addressed to the child at his/her address which is registered with the school as being his/her home address. **It should not be addressed or sent to the parent who made the request.** For further information, see "Important Note to Parents Making Access Requests on Behalf of their Child" below.

- In any of the circumstances outlined above, if the data contains health data and disclosure would be likely to cause serious harm to the physical or mental health of the individual concerned, the school is obliged to withhold the data until they have consulted with the data subject's medical practitioner and (in the case of a student under 18 or a student with special educational needs whose disability or medical condition would impair his or her ability to understand the information), parental/guardian consent should also be sought.
- In some cases (i.e. where the information is **"health data**"), it is advised that the data be supplied by the medical practitioner.
- In any of the circumstances outlined above, if the data contains **social work data** and disclosure would be likely to cause serious harm to the physical or mental health of the individual, the school is not permitted to release the data to the individual.

Note B: Exceptions to note: Data protection regulations prohibit the supply of:
- **Health data** to a patient in response to a request for access if that would be likely to cause serious harm to his or her physical or mental health. This is to protect the individual from hearing anything about himself or herself which would be likely to cause serious harm to their physical or mental health or emotional well-being. In the case of health data, the information can only be released after the school has consulted with the appropriate health professional (usually the data subject's GP).

- Personal Data obtained in the course of carrying on social work ("**social work data")** (personal data kept for or obtained in the course of carrying out social work by a Government department, local authority, the HSE etc) is also restricted in some circumstances if that would be likely to cause serious harm to the health or emotional condition of the data subject concerned. In the case of social work data, the information cannot be supplied at all if the school believes it would be likely to cause serious harm to the physical or mental health or emotional condition of the data subject. If the social work data includes information supplied to the school by an individual (other than one of the school's employees or agents) while carrying out social work, the school is not permitted to supply that information to the data subject without first consulting that individual who supplied the information**.**

The Data Protection Acts state that the following data is **exempt** from a data access request:
1. Section 5 of the Data Protection Act provides that the right of access does not apply in a number of cases in order to strike a balance between the rights of the individual, on the one hand, and some important needs of civil society on the other hand. Examples would include the need for state agencies (like An Garda Síochána) to **investigate crime** effectively and the need to protect the international relations of the State.
2. **Estimates of liability**: where the personal data consists of or is kept for the purpose of estimating the amount of the liability of the school on foot of a claim for damages or compensation and where releasing the estimate would be likely to prejudice the interests of the school in relation to the claim, the data may be withheld.

3. **Legally privileged information**: the general rule is that all documentation prepared in contemplation of litigation is legally privileged. So correspondence between the school and their solicitors in relation to a case against the school should not be disclosed to the claimant pursuant to a data access request.
4. Section 4 states that the right of access does not include a right to see **personal data about another individual,** without that other person's consent. This is necessary to protect the privacy rights of the other person. If it is reasonable for the school to conclude that redacting or omitting the particulars identifying the third party would both conceal the identity of the third party and enable the data to be disclosed (subject to the redactions), then the data could be disclosed with such redactions. However, if it is not possible to redact or omit the particulars which identify a third party, then the affected data should not be released to the applicant.

5. Section 4 also states that where personal data consists of **expressions of opinion** about the data subject made by another person, the data subject has a right to receive that expression of opinion **except** where that expression of opinion was given in confidence, and on the clear understanding that it would be treated as confidential.
6. The obligation to comply with an access request does not apply where it is impossible for the school to provide the data or where it involves a disproportionate effort.
Where a school refuses to hand over some or all of the personal data they hold in relation to a data subject (on the basis of any of the exemptions or prohibitions set out above), the school must advise the data subject of this in writing, setting out reasons for the refusal and notifying the data subject that he or she has the right to complain to the Office of the Data Protection Commissioner about the refusal.

Data Request Form

Heywood Community School

Access Request Form: Request for a copy of Personal Data under the Data

Protection Act 1988 and Data Protection (Amendment) Act 2003

Important: Proof of Identity must accompany this Access Request Form (eg. official/State photographic identity document such as driver's licence, passport).

A fee of €6.35 must accompany this Access Request Form if it is a Section 4 Data Access Request together with proof of identity (eg. official/State photographic identity document such as driver's licence, passport).

Full Name	
Maiden Name (if name used during your school duration	
Address	
Contact Number ≠	Email Address≠

≠ *We may need to contact you to discuss your access request*

Please tick the box which applies to you:

Student □	**Parent/Guardian of student** □	**Former Student** □	**Current Staff** □	**Former Staff** □
Age: **Year:** **Class:**	**Name of Student**	**Insert Year of leaving**		**Insert years From/To:**

Section 3 Data Access Request:

I, …… (insert name) wish to be informed whether or not Heywood Community School holds personal data about me/my child and to be provided with a description of this data and to be informed of the purpose for holding such data. I am making this request under **Section 3 of the Data Protection Acts.** ☐

OR

Section 4 Data Access Request:

I, ……..(insert name) wish to make an access request for the copy of any personal data that Heywood Community School holds about me/my child. I am making this access request under **Section 4 of the Data Protection Acts.** ☐

Section 4 Data Access only: I attach €6.35 ☐

Any other information relevant to your access request (e.g. if requesting images/recordings made by CCTV, please state the date,time,and location of the images/recordings (otherwise it may be very difficult or impossible for the school to locate the data)

Signed …….. Date:…….

Checklist: Have you:

1. **Completed the Access Request form in full?** ☐
2. **Included a cheque or postal order made payable to Heywood Community School in the amount of €6.35 where a section 4 request is made?** ☐
3. **Signed and dated the Access Request Form?** ☐
4. **Included a photocopy of official/State photographic identity documentation (driver's licence, passport etc)** ☐

   Note to school/ETB: *the school/ETB should satisfy itself as to the identity of the individual and make a note in the school/ETB records that identity has been provided, but the school/ETB should not retain a copy of the identity document*.

Please return this form to the relevant address: **The Principal, Heywood Community School, Ballinakill, Co. Laois**

Personal Data Security Breach Code of Practice

Heywood Community School

Purpose of Code of Practice: This Code of Practice applies to Heywood Community School as data controller. This Code of Practice will be:

1. available on the school website

2. circulated to all appropriate data processors and incorporated as part of the service-level agreement/data processing agreement between the school/ and the contracted company

3. shall be advised to staff at induction and at periodic staff meeting(s) or training organised by the school.

Obligations under Data Protection :The school as data controller and appropriate data processors so contracted, are subject to the provisions of the Data Protection Acts, 1988 and 2003 and exercise due care and attention in collecting, processing and storing personal data and sensitive personal data provided by data subjects for defined use.

The school has prepared a **Data Protection Policy** and monitors the implementation of this policy at regular intervals. The school retains records (both electronic and manual) concerning personal data in line with its Data Protection Policy and seeks to prioritise the safety of personal data and particularly sensitive personal data, so that any risk of unauthorized disclosure, loss or alteration of personal data is avoided.

Protocol for action in the event of breach

In circumstances where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the school/ETB will follow the following protocol:

1. The school will seek to contain the matter and mitigate any further exposure of the personal data held. Depending on the nature of the threat to the personal data Depending on the nature of the threat to the personal data, this may involve a quarantine of some or all PCs, networks etc. and requesting that staff do not access PCs, networks etc. Similarly, it may involve a quarantine of manual records storage area/s and other areas as may be appropriate. By way of a preliminary step, an audit of the records held or backup server/s should be undertaken to ascertain the nature of what personal data may potentially have been exposed.

2. Where data has been “damaged” (as defined in the Criminal Justice Act 1991, e.g. as a result of hacking), the matter must be reported to An Garda Síochána. Failure to do so will constitute a criminal offence in itself (“withholding information”) pursuant to section 19 Criminal Justice Act, 2011. The penalties for withholding information include a fine of up to €5,000 or 12 months’ imprisonment on summary conviction.

3. Where the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the school may conclude that there is no risk to the

data and therefore no need to inform data subjects or contact the Office of the Data Protection Commissioner. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

4. Depending on the nature of the personal data at risk and particularly where sensitive personal data may be at risk, the assistance of An Garda Síochána should be immediately sought. This is separate from the statutory obligation to report criminal damage to data arising under section 19 Criminal Justice Act 2011 as discussed at (2) above.

5. Contact should be immediately made with the data processor responsible for IT support in the school.

6. In addition and where appropriate, contact may be made with other bodies such as the HSE, financial institutions etc.

7. Reporting of incidents to the Office of Data Protection Commissioner: All incidents in which personal data (and sensitive personal data) has been put at risk shall be reported to the Office of the Data Protection Commissioner as soon as the school becomes aware of the incident (or within 2 working days thereafter), save in the following circumstances:

- When the full extent and consequences of the incident have been reported without delay directly to the affected data subject(s) **and**
- The suspected breach affects no more than 100 data subjects **and**
- It does not include sensitive personal data or personal data of a financial nature

Where all three criteria are not satisfied, the school shall report the incident to the Office of the Data Protection Commissioner within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident (see further details below). Where no notification is made to the Office of the Data Protection Commissioner, the school shall keep a summary record of the incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record shall comprise a brief description of the nature of the incident and an explanation why the school did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records shall be provided to the Office of the Data Protection Commissioner upon request.

8. The school shall gather a small team of persons together to assess the potential exposure/loss. This team will assist the Principal of the school (and the school's DP Compliance Officer) with the practical matters associated with this protocol.

9. The team will, under the direction of the Principal, give immediate consideration to informing those affected. At the direction of the Principal the team shall:

- Contact the individuals concerned (whether by phone/email etc.) to advise that an unauthorised disclosure/loss/destruction or alteration of the individual's personal data has occurred.

- Where possible and as soon as is feasible, the data subjects (i.e. individuals whom the data is about) should be advised of the nature of the data that has been potentially exposed/compromised;
- the level of sensitivity of this data and
- an outline of the steps the school intends to take by way of containment or remediation.
- Individuals should be advised as to whether the school intends to contact other organisations and/or the Office of the Data Protection Commissioner.
- Where individuals express a particular concern with respect to the threat to their personal data, this should be advised back to the principal who may, advise the relevant authority e.g. Gardaí, HSE etc.
- Where the data breach has caused the data to be "damaged" (e.g. as a result of hacking), the principal shall contact An Garda Síochána and make a report pursuant to section 19 Criminal Justice Act 2011.
- The Principal shall notify the State Claims Agency and advise them that there has been a personal data security breach. .

10. Contracted companies operating as data processors:

- Where an organisation contracted and operating as a data processor on behalf of the school/ETB becomes aware of a risk to personal/sensitive personal data, the organisation will report this directly to the school/ETB as a matter of urgent priority. In such circumstances, the Contact the individuals concerned (whether by phone/email etc.) to advise that an unauthorised disclosure/loss/destruction or alteration of the individual's personal data has occurred.

Further advice: What may happen arising from a report to the Office of Data Protection Commissioner?

- Where any doubt may arise as to the adequacy of technological riskmitigation measures (including encryption), the school shall report the incident to the Office of the Data Protection Commissioner within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact will be by e-mail, telephone or fax and shall not involve the communication of personal data.
- The Office of the Data Protection Commissioner will advise the school of whether there is a need for the school to compile a detailed report and/or for the Office of the Data Protection Commissioner to carry out a subsequent investigation, based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.
- Should the Office of the Data Protection Commissioner request the school to provide a detailed written report into the incident, the Office of the Data Protection Commissioner will specify a timeframe for the delivery of the report into the incident and the information required. Such a report should reflect careful consideration of the following elements:

- the amount and nature of the personal data that has been compromised
- the action being taken to secure and/or recover the personal datathat has been compromised

- the action being taken to inform those affected by the incident or reasons for the decision not to do so
- the action being taken to limit damage or distress to those affected by the incident
- a chronology of the events leading up to the loss of control of the personal data; and
- the measures being taken to prevent repetition of the incident.

Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where the school has not already done so. If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.

GDPR Records Retention Schedule for Heywood Community School

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

Records relating to pupils/students	C &C	Confidential shredding	Comments
Enrolment Forms	Student reaching 18 years +7 years	Confidential shredding	18 is age of majority plus 7 years (6 years in which to make a claim against the school, plus 1 year for proceedings to be served on the school)
Student Transfer forms (applies from primary to primary: from one second level to another)	Student reaching 18 years + 7 years	Confidential shredding	18 is age of majority plus 7 years (6 years in which to make a claim against the school, plus 1 year for proceedings to be served on the school)
Disciplinary notes	Never destroy	N/A	Never destroy
Results of in-schooltests/exams (i.e. end of term, end of year exams, assessment results)	Student reaching 18 years + 7 years	Confidential shredding	18 is age of majority plus 7 years (6 years in which to make a claim against the school, plus 1 year for proceedings to be served on the school
End of term/year reports	Student reaching 18 years +7 years	Confidential shredding	18 is age of majority plus 7 years (6 years in which to make a claim against the school, plus 1 year for proceedings to be served on the school)
Record of school tours/trips, including permission slips, itinerary reports	Never destroy	N/A	Never destroy
Scholarship applications e.g. Gaeltacht, book rental scheme	Student reaching 18 years +7 years	Confidential shredding	18 is age of majority plus 7 years (6 years in which to make a claim against the school, plus 1 year for proceedings to be served on the schoo
Garda vetting form & oiutcome- **Students**	Record of outcome retained for 12 months	Confidential shredding	Record of outcome retained for 12 months. School to retain the reference number and date of disclosure on file, which can be checked with An Garda Siochana in the future.

Sensitive Personal Data Students	C&C	Comments
Psychological assessments	Indefinitely	Never destroy
Special Education Needs' files, reviews, correspondence and Individual Education Plans	Indefinitely	Never destroy
Accident reports	Indefinitely	Never destroy
Child protection records	Indefinitely	Never destroy
Section 29 appeal records	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Enrolment/transfer forms where child is not enrolled or refused enrolment	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Records of complaints made by parents/ guardians	Depends entirely on the nature of the complaint.	Depends entirely on the nature of the complaint. If it is child-safeguarding, a complaint relating to teacher-handling, or an accident, then retain indefinitely. Never destroy. If it is a complaint of a more mundane nature (e.g. misspelling of child's name, parent not being contacted to be informed of parent-teacher meeting) or other minor matter, then student reaching 18 years + 7 years (6 years in which to take a claim, and 1 year for proceedings to be served on school)

Staff Records	Final disposition	Comments
Recruitment process Note: these suggested retention periods apply to unsuccessful candidates only. They do NOT apply to successful candidates, or candidates who are/were also employees already within your school applying for another post/position. For successful candidates, or candidates who are/were also employees already within your school applying for another post/position, see retention periods set out below.	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Applications & CVs of candidates called for interview	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Database of applications	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Selection criteria	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Applications of candidates not shortlisted	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Unsolicited applications for jobs	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Candidates shortlisted but unsuccessful at interview	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.

Board of Management Records	Final disposition	Comments
Board agenda and minutes	N/A	Indefinitely. These should be stored securely on school property
School closure		On school closure, records should be transferred as per Records Retention in the event of school closure/amalgamation. A decommissioning exercise should take place with respect to archiving and recording data.
Other school based reports/minutes	**Final disposition**	**Comments**
CCTV recordings	Safe/secure deletion.	28 days in the normal course, but longer on a case-by-case basis e.g. where recordings/images are requested by An Garda Síochána as part of an investigation or where the records /images capture issues such as damage/vandalism to school property and where the images/recordings are retained to investigate those issues.
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".
Financial Records	**Final disposition**	**Comments**
Audited Accounts	n/a	Indefinitely
Payroll and taxation		Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Note: The DES requires of 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.
Invoices/back-up records/receipts		Retain for 7 years

Promotion process	Final Disposition	Comments
Posts of Responsibility	N/A	**Retain indefinitely on master file as it relates to pay/pension etc. (See DES guidelines)**
Calculation of service	N/A	Retain indefinitely on master file
Promotions/POR Board master files	N/A	Retain indefinitely on master file
Promotions/POR Boards assessment report files	N/A	Retain original on personnel file in line with retention periods in "Staff Records" retention guidelines above
POR appeal documents	N/A	Retain original on personnel file, and copy of master & appeal file. Retain for duration of employment + 7 years (6 years in which to take a claim, plus 1 year to serve proceedings on school). Copy on master and appeal file.
Correspondence from candidates re feedback	N/A	Depends upon nature of feedback. If feedback is from unsuccessful candidate who is not an employee within the school, keep in line with retention periods in "Staff Records" above. If feedback is from successful candidate or from unsuccessful candidate who is already an employee within the school, keep in line with "Staff personnel while in employment" above.

Candidates shortlisted and are successful but do not accept offer	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Interview board marking scheme & board notes	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Panel recommendation by interview board	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.

Staff personnel files (whilst in employment)	Final Disposition	Comments
e.g. applications, qualifications, references, recruitment, job specification, contract, Teaching Council registration, records of staff training 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	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	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	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 (the section which relates to the employee only)	Confidential shredding	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	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	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)
Panel recommendation by interview board	Confidential shredding	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	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 specification/ description	Confidential shredding	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	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	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 and correspondence (whether successful or not)	Confidential shredding	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)
Leave of absence applications	Confidential shredding	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	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	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	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	Retain for 2 years following 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	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). There is a statutory requirement to retain for 8 years.
Force Majeure leave	Confidential	Retain for 8 years or the duration of employment plus 7 years (6 years in

	shredding	which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater). There is a statutory requirement to retain for 8 years.
Carers leave	Confidential shredding	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). There is a statutory requirement to retain for 8 years
Working Time Act (attendance hours, holidays, breaks)	Confidential shredding	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). There is a statutory requirement to retain for 3 years
Allegations/complaints	ETB one doesn't have a time period advised	Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served). **Please note** the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains "active" on an employee's record.

Superannuation /Pension /Retirement records	**Final Disposition**	**Comments**
Records of previous service (incl. correspondence with previous employers)	N/A	DES advise that these should be kept indefinitely.
Pension calculation	Confidential shredding	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 is the longer)

Government returns	**Final disposition**	**Comments**
Any returns which identify individual staff/pupils,	N/A	Depends upon the nature of the return. If it relates to pay/pension/benefits of staff, keep indefinitely as per DES guidelines. If it relates to information on students, e.g. October Returns, Annual Census etc., keep in line with "Student Records" guidelines above.
Pension increases (notification to Co. Co.)	Confidential shredding	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 is the longer)