

Bennekerry N.S.

Data Protection Policy



INTRODUCTORY STATEMENT

The school's Data Protection Policy applies to the **personal data** held by the school's Board of Management (BoM), which is protected by the Data Protection Acts 1988 to 2018 and the EU General Data Personal Regulation (GDPR)

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 special categories of personal data will be protected by the school.

Bennekerry N.S. operates a "**Privacy by Design**" method in relation to Data Protection. This means we plan carefully when gathering personal data so that we build in the **data protection principles** as integral elements of all data operations in advance. We audit the personal data we hold in order to

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

DATA PROTECTION PRINCIPLES

The school BoM 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 BoM is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 to 2018 and GDPR, which can be summarised as follows:

1. Obtain and process Personal Data fairly

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

2. Consent

Where consent is the basis for provision of personal data, (e.g. data required to join sports team/ afterschool activity or any other optional school activity) the consent must be a freely-given, specific, informed and unambiguous indication of the data subject's wishes.

Bennekerry N.S. will require a clear, affirmative action e.g. ticking of a box/signing a document to indicate consent. Consent can be withdrawn by data subjects in these situations.

3. Keep it only for one or more specified and explicit lawful purposes

The BoM will inform individuals of the reasons they collect their data and the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times.

4. Process it only in ways compatible with the purposes for which it was given initially

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

5. Keep Personal Data safe and secure

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

6. Keep Personal Data accurate, complete and up-to-date

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

7. Ensure that it is adequate, relevant and not excessive

Only the necessary amount of information required to provide an adequate service will be gathered and stored.

8. Retain it no longer than is necessary for the specified purpose or purposes for which it was given

As a general rule, the information will be kept for the duration of the individual's time in the school. Thereafter, the school will comply with DES guidelines on the storage of 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. See **School Record Retention** table.

9. Provide a copy of their personal data to any individual on request

Individuals have a right to know and have access to a copy of personal data held about them, by whom, and the purpose for which it is held.

SCOPE

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

The policy applies to all school staff, the 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:

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

Data Controller is the Board of Management of the school

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

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

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

Data Processor - a person who processes personal information on behalf of a data controller, but **does not include an employee of a data controller** who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection legislation places responsibilities on such entities in relation to their processing of the data. In Bennekerry N.S. we use Aladdin, School Accounting, Priority ICT, Horizon, AIB IBB Banking, Schoolwise, DES., Charity Regulator, NEPS, HSE, TUSLA.

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

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

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

RATIONALE

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

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. The school takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the 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. Some of these are directly relevant to data protection. **For example:**

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

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

Under **Section 20(5) of the Education (Welfare) Act, 2000**, a Principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the Principal of another school to which a student is transferring. Bennekerry N.S. sends, by post, a copy of a child's *Passport*, as provided by the National Council for Curriculum and Assessment, to the Principal of the Post-Primary School in which the pupil has been enrolled.

Where reports on pupils which have been completed by professionals, apart from Bennekerry N.S. staff, are included in current pupil files, such reports are only passed to the Post-Primary school following express written permission having been sought and received from the parents of the said pupils.

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

Under **Section 28 of the Education (Welfare) Act, 2000**, the School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, Tusla, the National Council for Special Education and other schools). The BoM must be 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; 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) 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 most schools are not currently subject to freedom of information legislation, (with the exception of schools under the direction of Education and Training Boards), 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 by that body if a request is made to that body.

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

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

RELATIONSHIP TO CHARACTERISTIC SPIRIT OF THE SCHOOL:

Bennekerry N.S. seeks to:

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

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

PERSONAL DATA

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

1. Staff records:

a) Categories of staff data:

As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:

- Name, address and contact details, PPS number.
- Name and contact details of next-of-kin in case of emergency.
- Original records of application and appointment to promotion posts
- Details of approved absences (career breaks, parental leave, study leave, etc.)
- Details of work record (qualifications, classes taught, subjects, etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties

- Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under Children First Act 2015
- Photographs and recorded images of staff members (including at school events and noting achievements) are managed in line with the Acceptable Usage Policy.

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
- and for compliance with legislation relevant to the school.
- photographs and recorded images of staff member are taken to celebrate school achievements, e.g. 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 Acceptable Usage Policy'

c) Location and Security procedures of Bennekerry N.S.

- a. Manual records are kept in a secure, locked filing cabinet or press only accessible to personnel who are authorised to use the data. Employees are required to maintain the confidentiality of any data to which they have access.
- b. Digital records are stored on password-protected computers with adequate encryption and firewall software. The school has the burglar alarm activated during out-of-school hours.

2. 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) are managed in line with the accompanying policy on school photography.
- Academic record – subjects studied, class assignments, examination results as recorded on official School reports
- Records of significant achievements
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Other records e.g. records of any serious injuries/accidents, etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- Records of any reports the school (or its employees) have made in respect of the student to State Departments and/or other agencies under Children First Act 2015.

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

- to enable each student to develop to his/her 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, e.g. 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 Acceptable Usage Policy*'.
- to ensure that the student meets the school's admission criteria
- to ensure that students meet the minimum age requirement for attendance at Primary School.
- to ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities
- to furnish documentation/information about the student to 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 second-level educational institutions.

c) *(Location and Security procedures as above):*

3. Board of Management records:

a) *Categories of Board of Management data:*

- 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 individuals.
- Photographs and recorded images of BoM members (including at school events and noting achievements) are managed in line with the Acceptable Usage Policy.

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.
- Photographs and recorded images of BoM members are taken to celebrate school achievements, e.g. 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 Acceptable Usage Policy'.

c) *(Location and Security procedures as above):*

3. Other Records: Creditors

a) *Categories of Board of Management data:*

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

- name
- address
- contact details
- PPS number
- tax details
- bank details and
- amount paid

b) *Purposes: The purposes for keeping creditor records are:*

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 and Security procedures as above):*

4. Other Records: Charity Tax-back Forms

a) Categories of Board of Management data:

The school may hold the following data in relation to donors who have made charitable donations to the school:

- name
- address
- telephone number
- PPS number
- tax rate
- signature and
- the gross amount of the donation.

b) Purposes: The purposes for keeping creditor records are:

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

c) (Location and Security procedures as above):

CCTV IMAGES/RECORDINGS-

CCTV is installed in Bennekerry N.S.

---a camera is installed externally covering the main entrance and a small section of the carpark in front of the office and staffroom windows.

--- cameras are installed internally covering the area inside the main front door and another covering the area inside the back door.

These CCTV systems may record images of staff, students and members of the public who visit the premises.

The viewing station is in the main school administration office

Purposes:

Safety and security of staff, students and visitors and to safeguard school property and equipment.

Security:

Access to images/recordings is restricted to the Principal and Deputy Principal of the school. Recordings are retained for 30 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to Data Protection Acts legislation.

EXAMINATION RESULTS

The school will hold data comprising examination results in respect of its students. These include class, mid-term, annual and continuous assessment results and the results of Standardised Tests.

Purposes:

The main purpose for which these examination results are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardian about educational attainment levels and recommendations for the future. 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 other schools to which pupils move.

Location and Security procedures

As above

LINKS TO OTHER POLICIES AND TO CURRICULUM DELIVERY

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

The following policies may be among those considered:

- Pupil Online Database (POD): Collection of the data for the purposes of complying with the Department of Education and Skills' pupil online database.
- Child Protection Procedures
- Anti-Bullying Procedures
- Code of Behaviour
- Enrolment Policy
- ICT Acceptable Usage Policy
- Assessment Policy
- Special Educational Needs Policy
- School Attendance Strategy
- Health and Safety Policy

PROCESSING IN LINE WITH A DATA SUBJECT'S RIGHTS

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

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

Data Processors

Where the school outsources to a data processor off-site, it is required by law to have a written contract in place. Bennekerry N.S. third party agreement specifies the conditions under which the data may be processed, the security conditions attaching to the processing of the data and that the data must be deleted or returned upon completion or termination of the contract.

Personal Data Breaches

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

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the BoM must communicate the personal data breach to the data subject without undue delay.

If a data processor becomes aware of a personal data breach, it must bring this to the attention of the data controller (BoM) without undue delay.

Dealing with a data 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.

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

No fee may be charged except in exceptional circumstances where the requests are repetitive or manifestly unfounded or excessive.

No personal data can be supplied relating to another individual apart from the data subject.

PROVIDING INFORMATION OVER THE PHONE

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

- Ask that the caller put their request in writing
- Refer the request to the Principal for assistance in difficult situations
- Not feel forced into disclosing personal information

IMPLEMENTATION ARRANGEMENTS, ROLES AND RESPONSIBILITIES

The BoM is the data controller and the Principal implements the Data Protection Policy, 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

RATIFICATION & COMMUNICATION

Ratified at the BoM meeting on *[Date]* and signed by Chairperson. Secretary recorded the ratification in the Minutes of the meeting

MONITORING THE IMPLEMENTATION OF THE POLICY

The implementation of the policy shall be monitored by the Principal, staff and the Board of Management

REVIEWING AND EVALUATING THE POLICY

The policy will be reviewed and evaluated after 2 years. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills or TUSLA), legislation and feedback from parents/guardians, students, school staff and others. The policy will be revised as necessary in the light of such review and evaluation and within the framework of school planning.

This policy was ratified by the Board of Management of Bennekerry N.S. at a meeting on 12th June 2018

Signed: Dea. Burke (*Chairperson of the Board of Management*)

Signed : Jonie Cleary (*School Principal and Secretary to the BOM*)

Appendix 1



Data Protection and COVID-19

“It is vital that schools have current lists of staff and pupils, by classes with contact telephone numbers for parents and guardians. These should be in Excel and ready to share with Department of Public Health, if required and requested under Infectious Diseases legislation, 1981, as amended. (Schools Pathway for Covid19, the Public Health Approach)

Governments, as well as public, private, and voluntary organisations are taking necessary steps to **contain the spread and mitigate the effects of COVID-19**, widely referred to as the ‘coronavirus’. **Many of these steps will involve the processing of personal data** (such as name, address, workplace, travel details) of individuals, including in many cases sensitive, ‘special category’ personal data (such as data relating to health).

Data protection law does not stand in the way of the provision of healthcare and the management of public health issues; nevertheless there are important considerations which should be taken into account when handling personal data in these contexts, particularly health and other sensitive data.

*Measures taken in response to Coronavirus involving the use of personal data, including health data, should be necessary and proportionate. Decisions in this regard will be informed by **the guidance and/or directions of public health authorities, or other relevant authorities.***

Bennekerry N.S. will have regard to the following obligations.

Lawfulness

There are a number of legal bases for the processing of personal data under Article 6 GDPR, and conditions permitting the processing of Special Categories of personal data, such as health data, under Article 9 that may be applicable in this context. Among these, the following may be relevant.

In circumstances where organisations are acting on the **guidance or directions of public health authorities**, or other relevant authorities, it is likely that Article 9(2)(i) GDPR and Section 53 of the Data Protection Act 2018 will **permit the processing** of personal data, including health data, once **suitable safeguards** are implemented.^[1] Such safeguards may include **limitation on access** to the data, **strict time limits** for erasure, and other **measures such as adequate staff training to protect the data protection rights** of individuals.

Employers also have a **legal obligation** to protect their employees under the Safety, Health and Welfare at Work Act 2005 (as amended)^[2]. This obligation together with Article 9(2)(b) GDPR provides a legal basis to process personal data, including health data, where it is deemed **necessary and proportionate** to do so. Any data that is processed must be treated in a **confidential manner** i.e. any communications to staff about the possible presence of coronavirus in the workplace should not generally identify any individual employees.

It is also permissible to process personal data to protect the vital interests of an individual data subject or other persons where necessary. A person’s health data may be processed in this regard where they are physically or legally incapable of giving their consent.^[3] This will typically apply only in emergency situations, where no other legal basis can be identified.

Transparency

Organisations processing personal data **must be transparent** regarding the measures they implement in this context, including the **purpose** of collecting the personal data and **how long it will be retained** for. They must provide individuals with information regarding the processing of their personal data in a format that is **concise, easily accessible, easy to understand**, and in clear and plain language.

Confidentiality

Any data processing in the context of preventing the spread of COVID-19 must be carried out in a manner that ensures **security of the data**, in particular where health data is concerned. The identity of affected individuals **should not be disclosed** to any third parties or to their colleagues without a clear justification.

Data Minimisation

As with any data processing, only the **minimum necessary amount of data** should be processed to achieve the purpose of implementing measures to prevent or contain the spread of COVID-19.

Accountability

Controllers should also **ensure they document any decision-making process** regarding measures implemented to manage COVID-19, which involve the processing of personal data.

Further Information

Further information on COVID-19, including guidance for employers and the general public, can be found on the website of the [Health Protection Surveillance Centre](#)

Those seeking **more detailed information** on Data Protection obligations can consult the guidance on the [basics of data protection](#), ensuring that any processing is in line with the [principles of data protection](#), and identifying the [legal basis](#) which justifies the processing of personal data.

The European Data Protection Board (EDPB) has also adopted a [statement on the processing of personal data in the context of the COVID-19 outbreak](#), which provides further guidance on the lawfulness of processing and the special rules regarding the use of location data to monitor, contain, or mitigate the spread of COVID-19.

Questions.

In answer to **questions** about how Bennekerry N.S. can ensure any measures carried out are compliant with data protection law; the following should be noted:

Can an employer require all staff and visitors to the building to fill out a questionnaire requesting information on their recent travel history concerning countries affected by the virus, and medical info such as; symptoms of fever, high temperature, etc?

As noted above, employers have a legal obligation to protect the health of their employees and maintain a safe place of work. In this regard, and in the current circumstances, employers would be justified in asking employees and visitors to inform them if they have visited an affected area and/or are experiencing symptoms.

Implementation of more stringent requirements, such as a questionnaire, would have to have a strong justification based on necessity and proportionality and on an assessment of risk. This should take into consideration specific organisational factors such as the travel activities of staff attached to their duties, the presence of vulnerable persons in the workplace, and any directions or guidance of the public health authorities.

There would be no data protection implications in bringing the HSE recommendations to the attention of staff and visitors if they have recently travelled to an affected area and/or are experiencing symptoms, and requesting that they take any appropriate actions.

Any questions about the appropriate measures that should be implemented to protect against COVID19 should be addressed to the public health authorities.

Can an employer request more specific details of their employee's illness on medical certificates in light of the situation in relation to COVID-19?

While employers have a legal obligation to protect the health of their employees, employees also have a duty to take reasonable care to protect their health and the health of any other person in the workplace. In this regard, employers would be justified in requiring employees to inform them if they have a medical diagnosis of COVID-19 in order to allow necessary steps to be taken.

However, it is important to keep in mind that the recording of any health information must be justified and factual, and must be limited to what is necessary in order to allow an employer to implement health and safety measures. Employers should follow the advice and directions of the public health authorities, which may require the disclosure of personal data in the public interest to protect against serious threats to public health.

Employees should follow the advice of their healthcare practitioners and the public health authorities in these circumstances, who will instruct them as to what they need to do if they present symptoms of COVID-19

Can an employer send employees home from work if they are confirmed to have the virus?

Employers have a duty of care to employees to provide a safe place of work, which may require them to exercise discretion regarding access to premises. In a situation where an employee has confirmed that they have COVID-19, advice should be sought as a matter of urgency from the public health authorities as to what steps should be taken.

The decision to send employees home from work is not a data protection matter and may have other consequences for employers relating to employment law e.g. entitlement to sick pay.

Can an employer disclose that an employee has the virus to their colleagues?

This should be avoided, in the interests of maintaining the confidentiality of the employee's personal data. For example, an employer would be justified in informing staff that there has been a case, or suspected case, of COVID 19 in the organisation and requesting them to work from home. This communication should not name the affected individual.

Disclosure of this information may be required by the public health authorities in order to carry out their function.



DATA RETENTION PERIODS FOR SCHOOLS

Pupil Related	Retention Periods
School Register/Roll Books Enrolment Forms Disciplinary notes Test Results – Standardised Psychological Assessments etc. SEN Files/IEPS/SSFs Accident Reports Child Protection Reports/Records S.29 Appeals	Indefinitely Hold until Pupil is 25 Years Never Destroy Hold until pupil is 25 Years Never Destroy Never Destroy Never Destroy Never Destroy Never Destroy
Interview Records	
Interview Board Marking Scheme Board of Management notes (for unsuccessful candidates)	18 months from close of competition plus 6 months in case Equality Tribunal needs to inform school that a claim is being taken
Staff Records	
Contract of Employment Teaching Council Registration Vetting Records Accident/Injury at work Reports	Retention for duration of employment + 7 years (6 years to make a claim against the school plus 1 year for proceedings to be served on school)
BoM Records	
BOM Agenda and Minutes CC TV Recordings Payroll & Taxation Invoices/receipts Audited Accounts	Indefinitely 28 days normally. In the event of criminal investigation – as long as is necessary Revenue require a 6-year period after the end of the tax year Retain for 7 Years Indefinitely
<p><i>Why, in certain circumstances, does the Data Protection Commission recommend the holding of records until the former pupil has attained 25 years of age?</i></p> <p><i>The reasoning is that a pupil reaches the age of majority at 18 years and that there should be a 6-year limitation period in which it would be possible to take a claim against a school, plus 1 year for proceedings to be served on a school. The Statute of Limitations imposes a limit on a right of action so that after a prescribed period any action can be time barred.</i></p>	