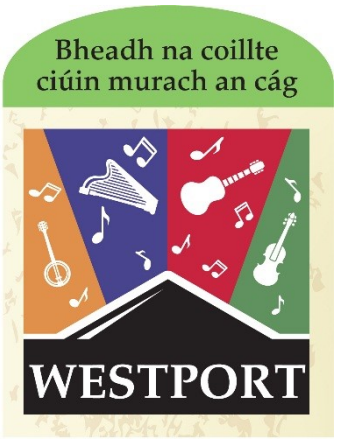

Data Protection Policy

Westport Scoil Cheoil

Introductory Statement

Westport Scoil Cheoil'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, participants (adult and child and others 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.

Westport Scoil Cheoil has at its core a desire to promote and protect the dignity of every member of its community, participants, tutors and guardians. This includes respect for the protection of data stored at the school and for the right of access to this data. This policy is informed by these aspirations and also the Data Protection Acts of 1988 and 2003, the General Data Protection Regulation of 2016 (GDPR) The policy applies to all WSC tutors, the Board of Management, parents/guardians, participants, (both adult and children) and their parents/guardians where applicable. The Board of Management of WSC is committed to the principles of responsible data protection as outlined in the documents referred to above and to this end it will: • obtain and fairly process personal data • keep data for one or more specified lawful purposes • process only data in ways compatible with the purposes for which it was given initially • securely store personal data • ensure that personal data is accurate and up-to-date • ensure that only relevant data is sought and stored • retain data no longer than is necessary for the specified purpose or purposes for which it was given • furnish a copy of personal data, or sensitive personal data to any individual, on request.

2.0:

Safeguarding Against Data Protection and Security Risks

This policy helps to protect WSC rom data security risks, including: • Breaches of security and confidentiality. For instance, information being given out inappropriately. • Reputational damage. For instance, WSC could suffer if hackers successfully gained access to sensitive data. • The risk of large fines or sanctions being imposed by the authorities. • The risks of being sued for damages by individuals whose data has been mishandled. Definitions as they pertain to this Policy For the purpose of this policy the following definitions apply:

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. Processing data refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations. 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. No Sensitive Personal Data is sought for WSC i.e. regarding a person's • racial or ethnic origin, political opinions or religious or philosophical beliefs • political opinions • religious or philosophical beliefs • trade union membership • genetic data • biometric data • physical or mental health condition • sexual orientation.

Data Controller refers to a person, company or body which determines the purposes and means of processing of personal data. The Data Controller for WSC College is the Board of Management.

4.0: Wider Legal Obligations

The provisions of this policy take cognisance of WSC's legal obligations and responsibilities in areas directly relevant to data protection, as outlined below: 1. Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School: this is done in each class each day. 2.Under Section 28 of the Education (Welfare) Act, 2000, WSC 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, centres of education) provided the School is satisfied that it will be used for a relevant purpose3. 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).

5.0:

What we use Personal Data for and what personal data we need

At Westport Scoil Cheoil the personal data records sought and retained by the school may include but are not limited to those listed below: 5.1: Student Records: It is the responsibility of parents/guardians and adult participants to inform WSC in WRITING of any relevant information that may affect their time at WSC (for example medical conditions etc). 5.1.2:These may include: • information which may be sought and recorded at enrolment and may be collated and compiled on the participants. These records may include: name, address and contact details, names and addresses of parents/guardians and their contact details.

All participants at WSC on enrolment will be counted as members of Westport Scoil Cheoil and shall remain so for 5 years unless we are notified in writing to the contrary. After 5 years all lists associated with WSC shall be destroyed/erased. This information shall only be used for WSC promotional and advertising purposes and for funding purposes such as from County/Town councils/ Department of Tourism/ Local Enterprises etc.

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).

The rationale for seeking and retaining student records is as follows: • to comply with legislative or administrative requirements • to enable parents/guardians to be contacted in the case of emergency or in the case of school closure.

to furnish documentation/ information about the participants to the Department of Education and Skills,/ education centre in compliance with law and directions issued by government departments • Participant data is kept both in manual form, within a relevant filing system and on computer files. Computer files require a password and WSC maintains the confidentiality of any data to which they have access. 5.2: Tutor records: It is the responsibility of tutors to inform WSC of any update to their personal data. 5.2.1: Categories of Tutor Data: These may include: • name, address and contact details, PPS number • 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 tutors to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures). •All tutors sign hard copies of MOU's to outline their legal obligations and their payment at WSC. These records are completely confidential and are stored in a locked filing cabinet in 'Ceol.' Only BOM members have access to this cabinet. These MOU's may be supplied to the Revenue Commissioners if requested to answer revenue queries in relation to tutors responsibility to pay their own taxes on income earned at WSC.

The rationale for seeking and retaining a staff member's personal data is as follows: • to facilitate the management and administration of WSC business • to facilitate the payment of tutors, and calculate other benefits/ entitlements where applicable (for example tutor accommodation) to manage human resources • to record promotions made (documentation relating to promotions applied for) and changes in responsibilities etc. • to enable WSC to comply with its obligations as an employer under the Safety, Health and Welfare at Work Act 2005 • to enable WSC to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies • for compliance with legislation relevant to the WSC. Tutor data maybe both in manual form, within a relevant filing system and/or on computer files hosted on secure cloud storage facilities. Computer files require a password and BOM membefrs are required to maintain the confidentiality of any data to which they have access.

5.3: Board of Management records:

5.3.1: 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) • Records in relation to appointments to the Board • Minutes of Board of Management meetings and correspondence to the Board that may include references to particular individuals. The rationale for seeking and retaining Board of Management data is as follows: • 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.

• Board of Management data is kept both in manual form, within a relevant filing system and on computer files. Computer files require a password and employees are required to maintain the confidentiality of any data to which they have access.

5.4: Creditors/Debtors 5.4.1: Categories of Creditors/Debtors Data: These may include: • name • address • contact details • PPS number • tax details • bank details • amount paid • amount owed. The rationale for seeking and retaining a creditor's/debtor's personal data is as follows: • This information is required for routine management and administration of the WSC's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

All financial transactions in relation to WSC are shared with our financial accountant firm Colm Mangan & Co Accountants Castlebar Co Mayo. They in turn share this information with Revenue /Returns each October.

6.0: Responsibilities and Compliance

Everyone who works for or with WSC has responsibility for ensuring data is collected, stored, and handled appropriately. Each person who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. Specific responsibilities are outlined in more detail below. 6.1: The Principal / Dr. Maura Thornton as Data Protection Officer (DPO) will • ensure that the basic principles of data protection are made available to tutors, participant and parents/guardians. This will be done on WSC website and also on-site during the Scoil Cheoil Week

The Board of Management as Data Controller will: • inform the person or persons involved, that a breach of confidentiality has occurred and that their personal data may have been compromised. • investigate where a breach of security has occurred and invoke appropriate action • review and update the Data Protection Policy if required. • ensure that only relevant data is processed • check to see if clerical and computer procedures are adequate to ensure accuracy. • reassure parents/guardians that the Data Protection Policy has been reviewed in tandem with the DPO, advise and inform employees of the need to work within the demands of the school's Data Protection policy.

WSC Data Processors will: • be required to sign off to confirm they have read and understand the Data Protection Policy and Procedures in their MOU. • check that any information that they provide in connection with their employment is accurate and up to date. • notify WSC of any changes to information they have provided, for example if they are not providing Revenue with their own tax returns. • ensure that personal information relating to students or their families is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.

Sanctions and Disciplinary Action Given the serious consequences that may arise, WSC may invoke appropriate disciplinary procedures for failure to adhere to the school's policy on Data Protection In the case of contractors or external service providers, serious breaches of the policies and procedures can and will be deemed grounds for termination of contractual agreements.

6.5: Compliance Monitoring and Review WSC will undertake regular reviews of internal procedures and changes in the legislation to ensure ongoing compliance with General Data Protection Regulation. This will include an annual review. 7.0: Data Security 7.1: Overview 1.

Access to data will be restricted to authorised tutors and BOM members on a “need-to-know” basis and where it is needed to fulfil their duties and responsibilities. 2. Data will not be shared informally. 3. WSC workers and tutors will keep all data secure by taking sensible precautions and following the guidelines below. 5. Strong passwords will be used, and never shared. 6. Personal data will not be disclosed to unauthorised people, either within WSC or externally.

7. Data will be regularly reviewed and if found to be out of date, will be deleted or disposed of after 5 years. 8. Tutors/ Workers/BOM will request help from the DPO or Data Controller if they are unsure about any aspect of data protection.

Data Storage The security of personal information relating to students and staff is a very important consideration under the Data Protection Acts and is taken very seriously at WSC. Appropriate security measures will be taken by the school to protect unauthorised access to this data.

A minimum standard of security will include the following measures:

Access to the information will be restricted to authorised WSC personnel on a “need-to-know” basis. • Manual files will be stored in a relevant filing system, located away from public areas. • Computerised data will be held under password protected files. • Any information which needs to be disposed of will be done so carefully and thoroughly. When data is stored on paper, it will be kept in a secure place where unauthorised people cannot see it. This also applies to data that is usually stored electronically but has been printed out for a valid reason: • When not required, the paper or files will be kept in a relevant filing system • All personnel will ensure that personal data, paper and printouts are not left where unauthorised people cannot see them. • Data will be shredded and disposed of securely when no longer required after 5 years. When data is stored electronically, it will be protected from unauthorised access, accidental deletion and malicious hacking attempts: • Data will be protected by strong passwords that are changed regularly and never shared between employees. • If data is stored on removable media (e.g. a USB key), these will be kept locked away (and ideally encrypted) when not being used. • Data will be stored on designated drives and servers and will only be uploaded to approved cloud computing services. • Servers containing personal data will be sited in a secure location. • Data will be backed up frequently. • All servers and computers containing data will be protected by an approved security software and a firewall.

7.3: Data Use Personal data is at often at the greatest risk of loss, corruption, or theft when it is being used or accessed: To mitigate this risk :- • when working with personal data, all personnel will ensure that the screens of their computers/tablets/apps are always locked when left unattended. • personal data shared by email will be downloaded, stored securely, and then deleted. • data will be encrypted before being transferred electronically where appropriate. •

7.4: Data Accuracy

WSC is cognisant of its duty to take reasonable steps to ensure that data is kept accurate and up-to-date. • Data will be held in as few places as necessary. • Every opportunity will be taken to ensure that data is updated. • WSC will make it as easy as possible for data subjects to update the information held about them, over the phone, or by email. • Data will be updated as and when inaccuracies are discovered (for example), if a data subject can no longer be reached on their stored telephone number, it will be removed from the database. 7.5: Data Disclosure to Third Parties As the Data Controller, the Board of Management is responsible for any personal data passed to third parties and care will be given to procedures and security.

Note: Data Collected Through Garda Vetting

WSC understands that sensitive information may be identified through Garda Vetting. In the event that a WSC tutor/helper Garda vetting raises concerns, the information will be dealt with on a confidential basis. All information pertaining to such a situation will be stored in the same way as other data. The Board of Management will not pass on a copy of a Garda Vetting Form to any other party.

8.0: Data Erasure and Disposal

When documentation or computer files containing personal data are no longer required, ie after membership of WSC has expired after 5 years the information will be disposed of carefully to continue to ensure the confidentiality of the data. Paper-based files and information no longer required, will be safely disposed of in shredding receptacles. Usually the data will be shredded on site by WSC personnel –In the case of personal information held electronically, temporary files containing personal information will be reviewed regularly and deleted when no longer required. When personal data reaches the point where the retention period has expired, the information will also be securely deleted and removed. In the event that IT equipment containing personal data is no longer required, all data stored on the devices will be removed prior to disposal. 9.0: Subject Access Request (SAR) Handling Procedure The Data Protection Acts, 1988 and 2003, the Data Protection Bill of 2018 and the 2016 GDPR provide for a right of access by an individual data subject to personal information held by WSC. A person seeking information, the Data Subject, is required to Data Protection Policy / to familiarise himself/herself with this policy. This may apply to a staff member or student seeking information on his or her own behalf or maybe a parent/guardian seeking information on behalf of his or her own son/daughter. No information will be supplied that relates to another individual. Although from time to time an individual may request by telephone details of some elements of their personal data, formal SARs must be submitted in writing, either electronically or by post.

9.1: Participants making access requests The Board of Management of WSC, in compliance with the GDPR recognises that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned, and also their rights in relation to the processing of personal data. It aims to balance the complementary rights of the child outlined in Articles 16(i) and 5 of the UN Convention of the Rights of the Child, these being that “no child shall be subjected to arbitrary or unlawful interference with his and her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour” and “rights and duties of parents to provide……. in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognised in the present Convention”. • Participants 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. Data Protection Policy 2018 2018 -Present 18 o If the information would be likely to be harmful to the individual concerned, parental/guardian consent will be sought before releasing the data to the student. • Each student request for Access to Personal Data will be assessed individually.

9.2: 9.5: Appealing a Decision in Relation to a Data Access Request

The Board of Management of WSC is respectful of the right of the Data Subject to appeal a decision made in relation to a request for data from this school. To appeal a decision, the Data Subject is advised to write to or email the Data Protection Commissioner explaining the case:- Canal House, Station Road, Portarlington, Co. Laois Data Protection. The correspondence should include: • the name of WSC • the steps taken to have concerns dealt with • details of all emails, phone calls, letters between the Data Subject and this school. 10: Data Breaches Definition: A data breach is an incident in which personal data has been lost, accessed, and/or disclosed in an unauthorised fashion. This would include, for instance, loss or theft of a laptop containing staff or student details, an email with personal information being sent to the wrong recipient, as well as more organised incidents of external hacking. All WSC personnel have a responsibility to take immediate action if there is a data breach. • If any personnel of WSC suspects at any time and for any reason that a breach may have occurred, then there is a need to report it to the DPO/Data Controller as an urgent priority • Once notification of an actual or suspected breach has been received, the DPO/Data Controller will put the Data Breach Procedure into operation with immediate effect.

10.1: Data Breach Handling Procedure The purpose of the Data Breach Procedure here below, is to ensure that all necessary steps are taken to: 1. contain the breach and prevent further loss of data 2. ensure data subjects affected are advised (where necessary) 3. comply with the law on reporting the incident to the Data Protection Commissioner if necessary 4. learn from the incident - identify what measures can and should be put into place to prevent similar occurrences in the future

10.2: Data Breach Response Plan • A Breach Incident Leader will be nominated. This person in WSC is the DPO. • Stakeholders will be identified • A breach response handling team will be formed - comprising WSC Management Team.The five-step process below will be initiated, with an evaluation after each stage The information communicated to data subjects will include information on the nature of the personal data breach and a contact point where more information can be obtained. It will recommend measures to mitigate the possible adverse effects of the personal data breach. The maximum timeframe for notification to the Office of the Data Protection Commissioner has been set at 72 hours from the time the incident is first discovered. 10.2.1: Data Breach – Five Step Process 1. Identification and Initial Assessment of the Incident. a. Identify and confirm volumes and types of data affected b. Establish what personal data is involved in the breach c. Identify the cause of the breach d. Estimate the number of data subjects affected e. Establish how the breach can be contained

2. Containment and Recovery a. Establish who within WSC needs to be made aware of the breach b. Establish whether there is anything that can be done to recover the losses and limit the damage the breach could cause c. Partial or complete systems lockdown d. Establish if it is appropriate to notify affected individuals immediately (for example where there is a high level of risk of serious harm to any individual) 3. Risk Assessment: A detailed analysis of volumes and types of data involved will be undertaken and a risk assessment carried out to establish

Risk Assessment: A detailed analysis of volumes and types of data involved will be undertaken and a risk assessment carried out to establish Data Protection Policy .Present a. risks for Data Subjects b. risks for the School 4. Notification a. On the basis of the evaluation of risks and consequences, the Breach Response Team will decide whether it is necessary to signal the breach outside of the school. For example: i. the Gardaí ii. the Data Subjects affected by the breach iii. the Data Protection Commissioner iv. the school's insurers In accordance with the Data Protection Commissioner's Code of Practice all incidents in which Personal Data has been

put at risk will be reported to the Office of the DPC within 72 hours of WSC first becoming aware of the breach. If, following the assessment described above, it is established that the data breach has been fully and immediately notified to the Data Subjects affected and it affects no more than 100 Data Subjects and it does not include sensitive personal data or personal data of a financial nature, it may not require to be notified to the ODPC. This will be assessed on an individual basis according to the WSC's policy on Data Breach above, and where there is any doubt, legal advice will be sought. 5. Evaluation and Response a. Following any serious Breach of Data incident, a thorough review will be undertaken by the response team and a report will be made to the Data Controller. This will identify the strengths and weakness of the process and will indicate what areas may need to improve.

The Board of Management ratified this policy

Signed: Signed: