
# Bridge Mills Galway Language Centre

# GDPR and Privacy Documentation 2025

## Clear Desk Policy **version 1.01**

**Purpose**

The purpose of a clear desk policy is to ensure that all sensitive/confidential materials of students, staff, intellectual property, and clients are removed from the staff workspace and locked away when the items are not in use or staff leaves his/her workstation.

**Objective**

To increase staff awareness about protecting sensitive/confidential information and personal data as part of standard basic privacy controls.

To empower staff within an organised environment and provide a good impression for clients of B

To reduce the threat of security to confidential information. That means everyone in Bridge Mills Galway Language Centre must protect documents and data from unauthorised access, internally and from outsiders.

**Scope**

Clear desk policy not only includes documents and notes, but also post-its, business cards, and removable media.

**Sensitive/Confidential Data**

Employees are required to ensure that all sensitive/confidential information in hardcopy and/or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

**Filing cabinets** containing restricted, confidential and/or sensitive information must be kept closed and locked when not in use.

**Keys** used for access to be restricted, confidential and/or sensitive information must not be left at an unattended desk.

**Printouts** containing restricted, confidential and/or sensitive information should be immediately removed from printers.

**Restricted, confidential and/or sensitive documents** should be shredded in the official shredder bins or placed in locked disposal bins daily.

**Storage devices *such as USB drives must be encrypted*** and kept in a locked drawer.

**Whiteboards and Flip Charts** containing confidential, restricted and/or sensitive information should be erased immediately on completion of the task.

At known extended periods away from your desk, such as a lunch break, working papers are expected to be placed in locked drawers.

**PC's and Laptops**

- PC screens must be locked, requiring PIN to unlock, when workspace is unoccupied.
- PC's must be shut down completely at the end of the work day.
- Laptops must be either locked with a locking cable or locked away when not in use.
- All data must be saved to server or cloud, no saving to local drives.

**Daily Operations**

Passwords must not be written down.

Clear your workstation before you go home that includes removing cups, dishes, glasses, etc.

Scanned paper items must be stored on the Server, not locally on workstations, paper items must be shredded where no longer required.

Avoid printing off emails to read them. This generates increased amounts of clutter and should be shredded immediately.

Go through items on your desk to make sure you need them, dispose of as appropriate.

Try to handle any piece of paper only once, act on it, file it, scan or shred it.

If in doubt - shred it.

If you are unsure of whether a duplicate piece of documentation should be kept - it will probably be better to place it in the shredder.

**Compliance**

Bridge Mills Galway Language Centre management will verify compliance to this policy through various methods, including but not limited to, periodic observations, internal and external audits, and feedback from appropriate consultants.

Any exception to the policy must be approved by the DPL of Bridge Mills Galway Language Centre in advance.

Any staff found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Data Breach Policy

**Purpose**
If personal data is inadvertently released to a third party without consent, this may constitute a breach of the General Data Protection Regulation (GDPR) (EU) 2016/679.

Data security breaches are increasingly common occurrences whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information expands, there are more emerging ways by which data can be breached.

Bridge Mills Galway Language Centre have in place a robust and systematic process for responding to any reported data security breach. This will ensure Bridge Mills Galway Language Centre can act responsibly and protect its information assets as far as possible.

Sometimes a breach of personal information/data security may occur because this personal information/data is accidentally disclosed to unauthorised persons or, lost due to a fire or flood or, stolen as result of a targeted attack or the theft of a mobile computer device.

The purpose of this policy is to ensure that a standardised approach is implemented throughout Bridge Mills Galway Language Centre in the event of a personal information/data breach.

**Scope**
The policy applies to all stakeholders, specifically including employees, students, service providers, contractors and third parties that access, use, store or process personal information on behalf of Bridge Mills Galway Language Centre.

Data breaches are defined in three categories:

- Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, personal data
- Integrity breach - where there is an unauthorised or accidental alteration of personal data
- Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

"Data breach" means 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. Bridge Mills Galway Language Centre. is

legally required under the Irish Data Protection Act 1988 to 2018 and the GDPR to ensure the security and confidentiality of the information/data it processes on behalf of its students and guardians, agents, host families, service providers and employees.

Bridge Mills Galway Language Centre is legally required under the General Data Protection Regulation (GDPR) (EU) 2016/679 to ensure the security and confidentiality of the information/data it processed on behalf of its students, and guardians, agents, host families, service providers and employees.

A data security breach is considered to be "any loss of, or unauthorised access to Bridge Mills Galway Language Centre's personal data". Examples of data security breaches may include but not limited to: -

- Loss or theft of personal data
- Loss of unencrypted equipment storing personal data
- Human error for example sending personal data to the wrong email address
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceit

## Roles and Responsibilities

**Responsibilities**
**Information users**
All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

**Data Owners**
Data Owners are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

**Contact:**
In the event of a breach the following must need to be contacted immediately: Patrick Creed, Director at Bridge Mills Galway Language Centre: director@galwaylanguage.com.
**Data Security Breach Reporting**
In the case of a personal data breach, staff must inform privacy Bridge Mills Galway Language Centre of the personal data breach immediately (given that Bridge Mills Galway Language Centre have only 72 hours to report the breach to the Data Protection Commissioner). Confirmed or suspected data security breaches should be reported promptly to Patrick Creed Director at Bridge Mills Galway Language Centre. The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. Where possible the incident report should be completed as part of the reporting process.
Details of the Personal Data Breach to be reported: -

- describe the nature of the personal data breach
- systems used
- classification of personal data lost
- details of when, where and how this personal data was lost

- including where possible, the categories and approximate number of data subjects concerned
- approximate number of personal data records concerned
- describe the likely consequences of the personal data breach

Once a data breach has been reported an initial assessment will be made to establish the severity of the breach.
All data security breaches will be centrally logged in the incident reporting system.

**Data Breach Management Plan**
The management response to any reported data security breach will involve the following four elements: -

1. Containment and Recovery
2. Assessment of Risks to the rights and freedom of those affected
3. Consideration of Further Notification of those affected
4. Evaluation and Response

The log should record the timeline of the incident management.

**Reporting to the Data Protection Commissioner**
In the case of a personal data breach, Bridge Mills Galway Language Centre should report to the Data Protection Commissioner within 72 hours after having become aware of it unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Data Protection Commissioner is not made within 72 hours, it shall be accompanied by reasons for the delay.
Any service provider processing personal data on behalf of Bridge Mills Galway Language Centre should notify Bridge Mills Galway Language Centre without undue delay after becoming aware of a personal data breach.
The following information should be provided about the personal data breach: -

- describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned
- communicate the name and contact details of the Data Protection Manager or other contact point where more information can be obtained
- describe the likely consequences of the personal data breach
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

Bridge Mills Galway Language Centre will document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.
Communication of a personal data breach to the affected individuals: -

- When the personal data breach is likely to result in a high risk to the rights and freedoms of the individuals affected, Bridge Mills Galway Language Centre will communicate the personal data breach to the individuals affected without undue delay
- The communication to the individuals affected will describe in clear and plain language the nature of the personal data breach
- Bridge Mills Galway Language Centre will provide the name and contact details of the Data Protection Manager, describe the likely consequences of

the personal data breach and describe the measures taken or proposed to be taken to address the mitigation of the data breach including, if appropriate, measures taken

Communication to the affected individual is not required if any of the following conditions are met: -

- Bridge Mills Galway Language Centre has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- Bridge Mills Galway Language Centre has taken subsequent measures which ensure that the high risk to the rights and freedoms of affected individuals is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the affected individuals are informed in an equally effective manner.

**Risk-based reporting approach**

Breaches only need to be notified to the supervisory authority if it is determined that there is a risk to the rights and freedoms of the individuals. An individual only needs to be notified if there is a high risk to their rights and freedoms. Bridge Mills Galway Language Centre should assign a risk categorisation to each data breach. In assessing the potential impact consider the nature of the breach, the cause of the breach, the type of data exposed, mitigating factors in place and whether the personal data of vulnerable individuals has been exposed. The levels of risk can be further defined below:

| Level | Detail | DPC | Individual |
|---|---|---|---|
| Zero | No risk to the risks and freedom on individuals | N/A | N/A |
| Low | The breach is likely to have a minimal impact on individuals | Report | N/A |
| Medium | The breach may have an impact on individuals but the impact is unlikely to be substantial | Report | N/A |
| High | The breach may have a considerable impact on affected individuals | Report | Report |
| Severe | The breach may have a critical, extensive or dangerous impact on individuals | Report | Report |

Factors which could be taken into account when determining the risk weighting are as follows:

- Type of data involved (Personal Data, Special Category Data, financial data)

- Number of data subjects affected
- Duration of data breach. For example, whether it was a once off breach or a prolonged breach
- Type of data subject (child, adult, individual with physical or mental incapacity)
- Likely impact of the breach. For example, could it be used for identity theft or fraud or damage the reputation of the data subject. The impact of certain types of data being disclosed (e.g., health) may cause much more distress to a data subject than other generic types of data.
- Probability of identifying the data subject on the basis of the data
- Mitigating factors which can reduce the risk. For example, if a device was lost the data could be encrypted so that it is inaccessible by a third party.

The DPC requires that risk weightings are applied to each breach.

**Breach by another party**

Data breaches may occur through other parties such as a Data Processor. When engaging with such parties it is important that the contract specifically provides that Bridge Mills Galway Language Centre is notified of the breach as soon as possible and is provided with the appropriate supports so that the breach can be fully investigated by Bridge Mills Galway Language Centre.

# Purpose

GDPR places onerous accountability obligations on controllers and processors to demonstrate compliance.

The purpose of the Data Protection Governance Framework is to ensure Bridge Mills Galway Language Centre has good governance in the management of personal data processed as a controller and a processor.

# Objective

To ensure personal data processed as a controller and/or a processer is monitored, controlled and recorded by the appropriate members of Bridge Mills Galway Language Centre throughout the lifecycle from creation, processing, storage, transmission, deletion and destruction of personal data. Privacy by design and data protection by default must be standard practice for processing all personal data within Bridge Mills Galway Language Centre.

To provide an accountability approach by: -

- Documenting policies and procedures to be implemented by all staff
- Building a culture of data protection in the School, office, and while transferring data
- Educating all staff to ensure data protection encompasses the whole lifecycle of data in use, in transit and in rest whether physical or logical
- Providing the infrastructure for ongoing, efficient data protection management
- Developing a data protection risk mitigation strategy (specifically for the individual)
- Embedding data protection risk management throughout Bridge Mills Galway Language Centre
- Empowering Partners and Managers to assume responsibility for ensuring maintenance of Accountability Framework.

# Scope

The scope of this policy is to cover all categories of personal data held on various data subjects including but not limited to: -

- Students
- Guardians
- Teachers
- Educational Partners
- Host Families
- Potential candidates for employment

- Employees
- Contractors
- Suppliers

Personal data is information relating to an identified or identifiable natural person ('data subject'). Identifiable natural person is one who can be identified, directly or indirectly, name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Any special categories of personal data are subject to a higher level of protection and require an additional lawful basis to meet the threshold for processing. These data categories include genetic, biometric and health data, as well as personal data revealing racial and ethnic origin, political opinions, religious or ideological convictions or trade union membership.

Vulnerable segments of the population require special protection, such as, for example, people with mental health issues, asylum seekers, children, the elderly, a patient, or in any case where a power imbalance in the relationship between the position of the data subject and the controller can be identified.

**7 principles to comply to**

- Lawful, Fair and Transparent - Ensuring valid obtaining and processing of personal data
- Purpose Limitation - Ensuring data is kept for one or more specified, explicit and lawful purposes
- Data Accuracy - Ensuring the data processed is accurate, complete and up-to-date
- Data Minimisation - Ensuring the data processed is adequate, relevant and not excessive
- Storage Limitation - Ensuring personal data is kept for no longer than necessary
- Integrity and Confidentially - Ensuring the safety & security of data
- Accountability - Ensuring correct records are maintained

## Data Protection Management

Bridge Mills Galway Language Centre will assign the management of personal data to the school director. This role will require the Patrick Creed, Director, Bridge Mills Galway Language Centre to report directly to the appropriate body monthly on GDPR 9or as required). The role will include: -

- Provide external training providers to inform Bridge Mills Galway Language Centre of their obligations under GDPR
- Coordinate the monitoring of compliance to GDPR with the assistance of external consultants and management
- Alert management when Data Protection Privacy Impact Assessments are required

- Report to management
- Being a member of the Data Breach committee

**Training**

Bridge Mills Galway Language Centre will implement a training programme covering data protection generally and the areas that are specifically relevant to their school.

**Senior Staff**

Bridge Mills Galway Language Centre will ensure all management and teachers are educated about their requirements under GDPR and the possible impact of non-compliance for Bridge Mills Galway Language Centre.

Bridge Mills Galway Language Centre will identify key senior management to support the data protection compliance programme.

**General Staff**

Bridge Mills Galway Language Centre will ensure all staff and teachers are provided with a training programme covering data protection generally. Also, the areas that are specifically relevant to their jobs, providing the new policies setting out to comply.

Bridge Mills Galway Language Centre has a policy that all staff and teachers should be trained on Data Protection and will also ensure refresher training is provided when required.

Attendance at all training courses is recorded.

**Privacy by Design**

Bridge Mills Galway Language Centre will adopt internal policies, Technical and Organisational Measures (TOM) to meet the principles of privacy by design and data protection by default. Bridge Mills Galway Language Centre will adopt internal policies and implement technical and organisational measures by: -

- Implementing pseudonymisation and encryption where feasible
- Data Minimisation
- Risk Management
- Integrating data privacy into IT policies, Data Retention and Deletion Policy
- Providing data subject transparency and access
- By developing access controls for confidentiality which provide that only personal data which is necessary for each specific purpose of the processing is processed during the retention period as informed to the data subject
- By developing access controls (roles-based) which provide that personal data is not made accessible to more individuals than necessary for the purpose
- Providing an audit trail of the access controls
- Ability to restore availability of and access to data in the event of an incident
- Regular test of the effectiveness of security measures

Bridge Mills Galway Language Centre 's data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only

- Processed by Bridge Mills Galway Language Centre on the basis of either a valid contract, consent, legal compliance or legitimate interest
- Protected against any unauthorised access or illegal processing by internal or external parties.

Bridge Mills Galway Language Centre's data will not be:

- Communicated to any unauthorised internal or external parties
- Stored for longer than required for the purpose obtained
- Transferred to organisations, states or countries outside the European Economic Area without adequate safeguards being put in place as required under Data Protection Law.

Bridge Mills Galway Language Centre's commitment to protect individual's data:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in data protection and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorisation etc.).

**Data Privacy Impact Assessment (DPIA)**

Bridge Mills Galway Language Centre will carry out privacy impact assessments where a type of processing is likely to result in a high risk for the rights and freedoms of data subjects in the following cases but not limited to this list: -

- in the event of a systematic monitoring of a publicly accessible area
- in the context of profiling on which decisions are based that produce legal effects
- in the event of implementing new IT which infringes on the data subject's rights
- in the event there is a change to the risks posed by the processing operations to personal data

Bridge Mills Galway Language Centre will have in place a process for determining whether a Data Privacy Impact Assessment (DPIA) is required. A DPIA will be embedded in all Business Cases presented to management for any proposed new projects.

If a DPIA is required, the following process will be conducted: -

- a systematic description of the processing operations and purposes of the processing
- an assessment of the necessity and proportionality of the processing operations
- an assessment of the risks to the rights and freedoms of data subjects
- if appropriate may seek the views of the affected data subjects
- measures envisaged to address the risks

Bridge Mills Galway Language Centre will consult the Supervisory Authority if a DPIA result is of a high level of risk where Bridge Mills Galway Language Centre cannot take measures to mitigate this risk.

**Demonstrating Consent**

Bridge Mills Galway Language Centre will have an audit trail for consent. This will demonstrate that consent was given when relying on consent as a ground for processing personal data. Given the nature of the services offered consent is predominately relied on prior to engagement letters signed by the student or parent/guardian at the enrolment stage.

Consent is recorded from all data with a clear record of what each individual data subject consented to: -

**Demonstrating Compliance to the data protection principles**

Bridge Mills Galway Language Centre will document all the current processing activities to provide a Personal Data Register Data Protection Register identifying: -

- Service Department and Service line
- Data Class and Data Category
- Process Name
- Purpose for processing
- Data category and Data class
- Controller/Processor/Both/Joint Controller
- Data Owners
- Lawful basis
- Data Accuracy Process
- Process Map where available
- Format of Data
- Recipients of Data
- Data shares internally and lawful bases provided
- Transfer methods
- Location of Data storage
- Retention Periods
- Data Access Controls
- Risk Management
- Transfers to Third Countries
- External Processor

Bridge Mills Galway Language Centre will update its current policies and procedures to ensure compliance to the principles. See Section Policy Section.

**Records to be maintained as a Data Controller**

Bridge Mills Galway Language Centre will: -

- clearly identify where personal data is processed within the company, including by third party processors
- provide the name and contact details of the Bridge Mills Galway Language Centre and any joint controller
- use the Personal Data Register to record details of
    - the purposes of the processing
    - a description of categories of data subjects and personal data
    - the categories of recipients of personal data
    - the details of transfers to third countries

- the time limits for erasure of different categories of data
- a general description of technical and organisational security measures taken

**Export of Personal Data**

Bridge Mills Galway Language Centre will review and map the international data flows and complete a transfer impact assessment if outside the EEA, including:

- data flows where Bridge Mills Galway Language Centre is exporting to a controller or processor outside of the EEA
- data flows Bridge Mills Galway Language Centre is importing as a processor or controller
- consider what existing data transfer mechanisms are in place and whether these continue to be appropriate.
    - Countries that are currently white listed remain so until a Commission review finds otherwise
        - Andorra, Argentina, Canada, Switzerland, South Korea, Faeroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, UK, Uruguay and New Zealand
- Standard Contract Clauses remain a valid mechanism for non-EEA transfers
- ensure that export obligations are flowed down through subcontractor chains and across to other controllers where required

**Budget**

Bridge Mills Galway Language Centre will allocate an annual budget for data protection compliance.

**Reporting**

Staff are required to report any data breaches to Patrick Creed, Director, Bridge Mills Galway Language Centre as soon as the data breach is discovering (regardless of the timing of the discovering any day of the week and any time of the day).

The Office Manager will report to all staff any new changes to GDPR and of any cyber treats or attacks as this information becomes known, also providing steps to take to avoid this occurring to Bridge Mills Galway Language Centre.

The Office Manager will report to management monthly of: -

- Internal incidences reported
- Internal breaches
- GDPR improvements implemented
- Status of current projects on GDPR
- Awareness and training process
- Relevant external breaches reported
- Updates to compliance
- DPIA's

The DPL will assess all data breaches reported in line with the data breach policy and if such a breach requires reporting to the Supervisory Authority, this will be approved by management.

**Reference to Polices & Procedures**

The following policies and procedures, contracts and handbook form part of Accountability Framework

- Data Protection Governance
- Employee Handbook
- Privacy statement
- IT Policies

**Appendix A Right to lodge a complaint with supervisory authority**

Every data subject has the right to lodge a complaint with a supervisory authority if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy.

**Appendix B Right to an effective judicial remedy against a supervisory authority**

[Client] will have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

Each data subject shall have the right to an effective judicial remedy where the supervisory authority does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged.

**Appendix C Right to an effective judicial remedy against a controller or processor**

Each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

Proceedings against a [Client] as a controller or a processor may be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

**Appendix D Representation of data subjects**

The data subject has the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf.

Member States may provide that any body, organisation or association as described in previous paragraph, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

**Appendix E Right to compensation and liability**

Any person who has suffered material or non-material damage as a result of an infringement of this Regulation has the right to receive compensation from the controller or processor for the damage suffered.

Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

A controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

Where a controller or processor has paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage.

Court proceedings for exercising the right to receive compensation shall be brought before the courts.

**Appendix F General conditions for imposing administrative fines**

Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this in respect of infringements of this Regulation shall in each individual case be effective, proportionate and dissuasive.

Administrative fines shall, depending on the circumstances of each individual case, be imposed. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: -

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected, and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures

(e) any relevant previous infringements by the controller or processor

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

(g) the categories of personal data affected by the infringement

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

(i) where measures referred to in corrective powers have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct or approved certification mechanisms and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

Infringements of the following provisions shall, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: -

(a) the obligations of the controller and the processor

(b) the obligations of the certification body

(c) the obligations of the monitoring body pursuant

Infringements of the following provisions shall, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent

(b) the data subjects' rights

(c) the transfers of personal data to a recipient in a third country or an international organisation;

(d) any obligations pursuant to Member State law

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority or failure to provide access in violation of corrective power.

Non-compliance with an order by the supervisory authority as referred to in corrective action, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

**Bridge Mills Galway Language Centre Garda Vetting Policy -Draft V1.00**

## Purpose

The purpose of this policy is to ensure Bridge Mills Galway Language Centre complies with GDPR aspects of the Garda Vetting process.

## Scope

The scope of this policy extends to the Garda Vetting process undertaken for employees and/or contractors of this organisation.

### Definition

Garda vetting is a background check completed by the National Vetting Bureau and is an important safeguard in protecting the safety and welfare of children and vulnerable adults. The Garda vetting procedure is set down in the National Vetting Bureau (Children and Vulnerable Persons) Acts 2012 to 2016 ('the Acts') and is operated by The National Vetting Bureau ('NVB') of An Garda Síochána.

### The Vetting Process

Under the Acts, anyone who works with or undertakes an activity, of which a necessary and regular part of it consists of having access to or contact with children or vulnerable adults, is required to be vetted. This includes staff, volunteers and those on student placement working for a relevant organisation. A relevant organisation is an organisation that employs or permits a person to carry out work or activities, which mainly consist of them having access to, or contact with, children or vulnerable persons.

For the purposes of the Acts, a child is someone under the age of 18 and a vulnerable adult is any person (other than a child) who is suffering from a mental illness or a dementia, or has an intellectual disability, or is suffering from a physical impairment or disability which results in that person needing assistance for daily living activities or restricts that person's ability to protect himself or herself from others.

Bridge Mills Galway Language Centre is deemed a relevant organisation and is therefore registered with the NVB. The NVB will only conduct vetting for relevant organisations that are registered with them for vetting purposes. Once registered, as required we have appointed a liaison person. The liaison person makes vetting applications to the NVB and receives the vetting disclosures. For vetting to occur, individuals must complete a formal Garda Vetting Application Form and give written authorisation to An Garda Síochána to disclose to our organisation details of all prosecutions, successful or not, pending or completed and/or details of all convictions, recorded in the State or elsewhere or "specified information" in respect of them held on record by An Garda Síochána.

**E-Vetting**

Where we sign up for e-Vetting, an individual undergoing vetting is required to provide proof of identity to our nominated liaison person which must then be validated before the completion of the online vetting application.

**Information that may be disclosed as part of the vetting process**

A vetting disclosure to a relevant organisation will include details of a vetting subject's criminal record (if any), which will include a record of any convictions, within or outside the state, for any criminal offence, as well as details of any ancillary or consequential orders made as a result of the conviction. The record will also include any pending criminal prosecutions against the person whether within or outside the state.

Convictions for certain minor offences in the District Court that are over seven years old, which are set out in section 14A of the Acts, will not be disclosed. This does not apply to offences that are specified in Schedule 3 of the Acts and in Schedule 1 of the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016.

A vetting disclosure can also include details of "specified information" which is information concerning a finding or allegation of harm received by the NVB from the Garda Síochána or a Scheduled Organisation pursuant to section 19 of the Acts. 4 The information must reasonably lead to a bona fide belief that the vetting subject poses a threat to children or vulnerable people.

If specified information is found, the vetting subject will be informed and told of the NVB's intention to disclose the specified information. They will be given a summary of the relevant information and an opportunity to make a written submission in relation to the specified information. A determination will then be made as to whether the specified information will be disclosed. Upon making such a determination, there must be a bona-fide belief that the vetting subject poses a threat to children or vulnerable adults. The NVB must also be satisfied that the disclosure is reasonable, necessary and proportionate.

**Dispute Resolution**

All relevant organisations participate in a dispute resolution procedure designed to address any instance in which a vetting subject disputes the details contained in the relevant Garda Vetting disclosure. The procedure may be activated by the vetting subject by indicating the basis of their dispute in writing to the liaison officer who 4 For a full definition see Section 2 of the National Vetting Bureau (Children and Vulnerable Persons) Acts 2012 to 2016. 5 Pursuant to section 18 of the Acts, a vetting subject can appeal the decision to disclose specified information. Version Last Updated April 2021 3 received the Garda vetting disclosure. The liaison officer then resubmits the complete application file to the NVB for the conduct of further checks.

**Age**
If a candidate under the age of 18 requires vetting, (e.g. to enter a childcare course in college) permission from a parent or guardian is sought by An Garda Síochána prior to the individual undergoing vetting.

**Re-Vetting**
We may request individuals to undergo re-vetting after a suitable period of time has passed. This is also foreseen in the Acts. Section 20 provides for the re-vetting of employees and volunteers of specified organisations after a certain period. However, this section has not yet been commenced and the time-period has yet to be set down in regulations.

Re-vetting ensures that only suitably qualified persons undertake work or activities with children or vulnerable adults. It is also consistent with the data protection requirement that personal data is accurate and kept up to date, particularly in situations where new information come to light that points to a substantive and immediate risk to children or vulnerable adults.

**The processing of personal data contained in vetting disclosures**
We ensure that we are processing the personal data contained in a vetting disclosure in accordance with data protection law, and in particular with data protection principles. Some of the most relevant provisions are set down below.

**Lawful basis for processing personal data relating to vetting disclosures**
The lawful basis for any processing of personal data we undertake in relation to the vetting process is based upon Article 6(1)(c) when "necessary for compliance with a legal obligation to which the controller is subject". Organisations are required under the Acts to carryout Garda Vetting on individuals working with or undertaking an activity, of which a necessary and regular part of it consists of having access to or contact with children or vulnerable adults.

Where we process special categories of personal data, we will also identify a lawful basis under Article 9 GDPR.

Organisations processing personal data contained in a vetting disclosure will also include personal data relating to criminal convictions and offences. This includes:

- Personal data relating to a criminal conviction or offence
- Alleged offences/ unproven allegations; (including potentially specified information)
- Any proceedings in relation to an alleged offence
- Information relating to the absence of convictions

In such instances, we will only process criminal offence data if the processing is either under the control of official authority or authorised by EU or member state law. Section 55(1)(b)(v) Data Protection Act 2018 provides that the processing of criminal offence data is permitted when authorised by the law of the State. This would include Garda Vetting as foreseen under the Acts.

Section 55(1) Data Protection Act 2018 requires that the processing of personal data in respect of criminal convictions and offences is subject to "suitable and specific measures" being taken to safeguard the fundamental rights and freedoms of data subjects. Section 36 Data Protection Act 2018 sets out some suitable and specific measures a data controller may take to safeguard the fundamental rights and freedoms of data subjects. This means that we as a relevant organisation must take suitable and specific measures to safeguard the personal data of individuals undergoing vetting. Some relevant measures include:

- Limitations on access to the personal data undergoing processing within a workplace
- Strict time limits for the erasure of personal data and mechanisms to ensure that such time limits are observed
- Targeted training for those involved in the processing
- The appointment of a Data Protection Officer where it is not mandatory under the GDPR
- Logging mechanisms to permit the verification of whether and by whom the personal data have been consulted and/or erased.

With respect to any further processing, it is an offence for our organisation to use or disclose information contained within a vetting disclosure in a manner that is not foreseen by the Acts.

**The use of information received by** Bridge Mills Galway Language Centre
In accordance with the data protection principle of purpose limitation set down in Article 5(1)(b) GDPR, vetting disclosures may only be used for the purpose for which they were provided to [Organisation]'s and vetting disclosures should not be shared with any other organisation. The sole exception to this is where we have a joint employment agreement in writing in accordance with Section 12(3A) of the Acts.

It is also noted that under the Acts, Bridge Mills Galway Language Centre must receive a vetting disclosure for every individual undertaking relevant work or activities on behalf of Bridge Mills Galway Language Centre. As mentioned, it is also an offence for Bridge Mills Galway Language Centre to use or disclose information contained within a vetting disclosure in a manner that is not foreseen by the Acts.

**Secure storage of vetting information**
In accordance with the principle of integrity and confidentiality set down in Article 5(1)(f) GDPR, vetting disclosures will be held in a secure manner with access restricted to essential authorised personnel. This is particularly important given that the disclosures may contain special categories of personal data and/or personal data relating to criminal convictions and offences.

**Retention of vetting information**
In accordance with the principle of storage limitation, personal data will be destroyed when the purpose for which it was sought has expired. Vetting disclosures and all accompanying information such as identity documentation submitted as part of the vetting application will be routinely deleted, such as one year after they are received, unless Bridge Mills Galway Language Centre's has a compatible lawful purpose for retaining the information. In order to demonstrate compliance with

the Acts and in case of future queries in relation to a vetting disclosure, the reference number and date of disclosure can be retained on file which can be checked with the NVB.

With regard to all unsuccessful employment applications, the vetting disclosure and all other personal data collected in the recruitment process will not be kept beyond the statutory period in which a claim arising from the recruitment process may be brought. Bridge Mills Galway Language Centre's will include the retention periods for vetting applications, or the criteria used to determine that period in our data protection notices.

**Data subject rights**

Individuals also have a right to make a subject access request to receive a copy of their personal data from Bridge Mills Galway Language Centre's.

If, following the receipt of a Garda Vetting disclosure, a data subject believes that some of the information captured therein is inaccurate, they have a right to request the rectification of their personal data under the LED, which applies to matters of fact. This request should be made to An Garda Síochána and not the NVB. For example, if there is an inaccuracy in the details of a criminal conviction, a data subject can ask that this is rectified. This is in addition to the dispute resolution and appeal procedures foreseen in the Garda Vetting process.

However, this right is not absolute and in instances whereby it is not possible to ascertain whether the data is accurate, or where the personal data is required as evidence in proceedings before a court or tribunal or in another form of official inquiry, the Gardaí are required to restrict the processing of the data and shall not rectify the data. The right may also be restricted where it is considered necessary and proportionate in order to:

- avoid obstructing an official or legal inquiry, investigation or procedure
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties
- protect public security
- protect national security
- protect the rights and freedoms of others

## Bridge Mills Galway Language Centre Company System Policy Version 1.01

The objective of this policy to state what equipment usage is accepted to all employees and contractors using the equipment of Bridge Mills Galway Language Centre.

### Purpose

To provide of this policy to be provide clear guidance on the acceptable, safe and legal way in which Staff, contracts and board of management can use the organisations computing and networking service, as well as access to communications devices. By using any of the organisation's IT and Network Resources, you agree to comply with the terms of this Policy.

### Scope

This Policy covers:

- The organisations' Information Assets
- The organisations' IT and Network Resources (accessed on site or remotely) and/or communications devices

All information assets, IT and Network Resources equipment own by the organisation is referred to below as our IT resources.

You should be aware that Bridge Mills Galway Language Centre will monitor all the organisation owned devices, communications and downloads that pass through its facilities to safeguard the network. Should an investigation be required, Bridge Mills Galway Language Centre will first investigate other, less invasive, means to protect the confidentiality of data and the security of the network. Any information retained on Bridge Mills Galway Language Centre facilities may be disclosed to the Gardai if a valid request is presented. If there is evidence that you are not adhering to the guidelines set out in this policy, Bridge Mills Galway Language Centre reserves the right to take disciplinary action up to and including dismissal and/or legal action.

This Policy is based on the following principles:

1. Users must use our IT resources in a responsible, safe and lawful manner.
2. Users must respect the integrity IT resources

3. Users must only use our IT resources for the purpose of conducting your duties. We respect your privacy.

Users must not use our IT resources to:

1. Other than in the course of performing their duties, knowingly access, download or distribute illegal or inappropriate material, including material that is in any way pornographic, obscene, abusive, racist, libellous, defamatory or threatening.
2. Engage in any form of bullying or other behaviour which is illegal or likely to cause harassment to others.
3. Use social media to degrade, bully or intentionally offend Staff, Contractors or board of management
4. Gain unauthorised access to the account, systems or equipment of any third party - attempts at 'hacking' may result in criminal prosecution in Ireland or elsewhere.
5. Use another Users account.
6. Perform any activities which contravene the laws of the State, or the destination country in the case of data being transmitted abroad.
7. Undertake commercial activities or to otherwise further commercial objectives which are not a part of your duties
8. Infringe the copyright, patent or other intellectual property rights of any person including, by downloading unlicensed software or other unauthorised materials.
9. Access, modify, or interfere with computer material, data, displays, or storage media belonging to the organisation, except with their permission.
10. Connect unauthorised equipment to the network.
11. Load or execute unlicensed software or other material on our IT Resources where this is likely to breach the licensing conditions or other Intellectual Property rights.
12. Knowingly introduce any virus, malware or other destructive program or device into the systems or network.
13. The User should take all reasonable steps to ensure that they do not inadvertently introduce such programs or devices into the systems or network.
14. Use the network or equipment of personal use without prior authorisation

## Bridge Mills Galway Language Centre - E-Mail Signature Version 1.01

To replace the existing email confidential clause.

IMPORTANT DISCLAIMER – CONFIDENTIAL
This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the named addressee you should not disseminate, distribute or copy this email. Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. The opinions/views/comments on this email are those of the senders and do not necessarily reflect any views or policies of Bridge Mills Galway Language Centre. No liability is accepted by Bridge Mills Galway Language Centre for changes made to this message after it was sent or any losses caused by viruses contracted during transit over the Internet or present in any receiving system. This email is not intended to create legally binding commitments on behalf of Bridge Mills Galway Language Centre. The content of this email sent from and to this address may be viewed by other members of Bridge Mills Galway Language Centre where appropriate. This email is solely for business communication purposes and is therefore not intended to process personal data, save for HR purposes within Bridge Mills Galway Language Centre.  Bridge Mills Galway Language Centre is registered in Ireland, our registration number is 450520 and our registered address is The Bridge Mills, Galway, H91 R1WF, Ireland.

Bridge Mills Galway Language Centre Joiners, Mover, leavers Policy Version 1.01

## Joiners, Movers, Leavers (JML) Access Policy

The Joiners, Movers, Leavers (JML) Access Policy outlines the guidelines for managing user access to organisational systems, applications, and data during various employment stages: joining, moving within the organisation, and leaving the organisation. This policy ensures data security, compliance with privacy regulations, and efficient access management, Joiners, Movers, Leavers Procedure].

**Joining**

- Access Request
  Upon joining, operations manager initiates an access request for the new employee. The request includes the necessary system, application, and data access.
- Onboarding Process
  Academic and training manager/operations manager to provide a list of the relevant access based on the employee's role and responsibilities and send instructions to Zenotec.
- Access Review
  Within the first week, access is reviewed to ensure the employee has appropriate permissions and to remove any unnecessary access.
- Access Termination
  If the employee leaves during the probationary period, access is terminated immediately.

**Moving**

- Access Review
  Whenever an employee changes roles or departments, an access review is conducted to ensure access aligns with the new responsibilities.
- Access Adjustment
  Academic and training manager/operations manager based on instructions received will update access permissions based on the employee's new role and requirements.
- Previous Access
  Any unnecessary access from the previous role is promptly removed to prevent unauthorized use.

**Leaving**

- Access Termination Request
  When an employee resigns, access termination is requested by Academic and training manager/operations manager to Zenotec. If an employee is terminated, the access termination request is initiated immediately.
- Access Termination Process
  IT disables the employee's access to all systems, applications, and data upon receiving the request. This is done promptly to prevent unauthorised access.
- Exit Checklist
  Access termination is part of the exit checklist to ensure that no access is retained after departure.

**Data Protection**

- Data Ownership
  Access rights are granted based on the principle of least privilege, ensuring that employees have access only to the data they need to perform their duties.
- Confidential Data
  Special care is taken when granting access to sensitive and confidential data. Access is restricted to authorized individuals only.

**Staff WIFI Access**
The staff network is only available for Bridge Mills Galway Language Centre staff members.

**Guest WIFI Access**
The Guest network should be used by staff for mobile phone access and by third parties providing services directly to students and guests. Students and Guests will never have access to the staff network.

**Leaving policy-** To retrieve any personal data and update social media

**Information Security and Return of Bridge Mills Galway Language Centre Property**

Terminating employees are required to return to their manager all Bridge Mills Galway Language Centre owned property, equipment and materials which were issued to them during their employment. These items shall be returned on or before the last day of the individual's employment.

Your manager or other responsible administrators shall determine a date to revoke access rights to various Bridge Mills Galway Language Centre property and information, including but not limited to building access, computer systems, accounts and information access privileges on or before the date of termination.

**Retrieval of any personal data from devices**

Terminating employees who have downloaded Bridge Mills Galway Language Centre data including personal data onto their own devices must delete all data on or before termination of employment. This may include but not limited to smart phones/tablets/USB's/iPads/home computers or any other personal device used to access Bridge Mills Galway Language Centre data.

**Retrieval from your personal backups**

The deletion includes backups stored in the cloud/hard drives/or other storage devices such as USB's.

**Private Email Accounts**

Should an employee at any stage of employment email Bridge Mills Galway Language Centre data to their personal email account, this data must be deleted from your personal account before the date of termination.

It is the terminating employee's duty to ensure they fully delete all Bridge Mills Galway Language Centre data from personal emails, history files, devices and backups before date of termination.

**Refusal of deletion of Bridge Mills Galway Language Centre Property included data**

Refusal to return to Bridge Mills Galway Language Centre of any personal data processed by Bridge Mills Galway Language Centre may be construed as theft and appropriate legal action taken.

**Social Media**

On date of termination, the terminating employee must remove any reference to current employment in Bridge Mills Galway Language Centre ensuring all social media sites state your employment with Bridge Mills Galway Language Centre terminated on the agreed date.

**Confirmation of return of Organisations Property and Data**

Ensure there is an audit trail from each employee on termination of employment from Bridge Mills Galway Language Centre to validate the return of all the organisations property including personal data.

**Email Policy**

**Preparing an email**

While using emails to communicate, always construct emails in a professional manner, ensure that the “To” “CC” and BC boxes are left blank, while typing the mail content, so that the message is not sent accidentally. Type the recipient’s email address only after the mail has been written, checked and accepted.

Always start with a greeting e.g., Good Morning, good afternoon. The best way to decide how to address the recipient is to follow the way he/she addresses you e.g., Christian name or Mr/Ms and Surname. The main body of the email should be short and to the point. Complimentary Closing-Mails should end with “Thanks and regards” or “Best regards”.

Always consider who you are sharing your personal data with. Only share sensitive personal data (such as health data, IBAN) with trusted authorised recipients via a password protected file where the password is sent via text/SMS or sharepoint.

Before pressing send, double-checking addresses and attachments.

**Email Signature**

IMPORTANT DISCLAIMER – CONFIDENTIAL

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the named addressee you should not disseminate, distribute or copy this email. Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. The opinions/views/comments on this email are those of the senders and do not necessarily reflect any views or policies of Bridge Mills Galway Language Centre. No liability is accepted by Bridge Mills Galway Language Centre for changes made to this message after it was sent or any losses caused by

viruses contracted during transit over the Internet or present in any receiving system. This email is not intended to create legally binding commitments on behalf of Bridge Mills Galway Language Centre. The content of this email sent from and to this address may be viewed by other members of Bridge Mills Galway Language Centre where appropriate. Bridge Mills Galway Language Centre is registered in Ireland, our registration number is +353 91 566 468 and our registered address is The Bridge Mills, Galway, H91 R1WF, Ireland.

Your Email Signature should be set up from ALL devices used to access and write emails.

**Group emails**

Use “CC” for all internal Bridge Mills Galway Language Centre assigned email addresses.

Use “CC” for external email, where it is transparent that the external email address is used within an approved organisation and there is a legitimate reason to share the external email address with a relevant external individuals.

To avoid a personal data breach, use “BCC” in external emails (outside of Bridge Mills Galway Language Centre), where the email is going to more than one external *private* email address.

**Reply to all**

It is not always appropriate to “Reply to ALL”. Consider is it necessary to send your message to the author or to everyone on the list before selecting “Reply to ALL.

- Be careful when pressing Reply to ALL
- 'To' or 'Cc' allows recipients to **'Reply** all' which presents risks to disclose additional, possibly sensitive, personal information by the recipients themselves.

**Threads**

For each new email subject, start a new thread. Never reply to an old email relating to a different subject. Always provide a subject title for each email. The subject should be brief and to the point.

**Email sent in error**

- Once an email is sent to the wrong person report the error to the Data Protection Officer immediately
- If there is no risk to the rights and freedoms of the affected individuals
  The author should Bcc a follow up email to affected individuals apologizing, instructing that the offending email should be deleted, and advising recipients that they do not have the right to further use the email addresses identified to them.
- If there is risk to the rights and freedoms of the affected individuals, the Data Protection Officer will provide you with instructions subject to the type of personal data breached

**Timing of email**

In general emails should be sent during normal business hours. This is to respect people's Right to Disconnect if it is not urgent. If your role involves working outside normal business hours, you should send all standard emails to employees of Bridge Mills Galway Language Centre who are not on same shift and/or to external organisations using the time delay. If the email is urgent, send it immediately, regardless of day or time. However, always use the phone in the event of a critical incident.

**Out of office**

It is your duty to set "Out of office" when you are away and when you do not have access to your emails.
Thank you for your email. I am away from [day and date] to [day and date]. In my absence, please contact [Name, title, email address]. Kind regards [Full Signature].

**Monitor your emails**

It is your responsibility to monitor your emails.

**Forwarding a chain**

Instead of just forwarding emails, always try to cut and paste the relevant information to avoid unnecessary breaches of information.

Only forward an email to authorised personnel within Bridge Mills Galway Language Centre where it is necessary. Never forward emails externally to a third party unless it is authorised as part of your role.

Never forward Bridge Mills Galway Language Centre work emails to your private email account.

**Training**

Training is provided by Bridge Mills Galway Language Centre in various forms from attendances on courses, to communications provided on changes to policies and procedures. It is your duty to keep up to date with all training provided and ensure that new changes are implemented as part of your role.

**Be wary of the following.**

- links that are forwarded by email, particularly if you're not expecting such links or you think it has been automatically forwarded, as this is a common way to spread malicious links.
- avoid clicking links or opening attachments that you are unsure about. In particular, be wary of attachments which you were not expecting. Keep in mind that displayed text for a link can look like a legitimate URL, but the link when you click it may lead somewhere else.
- Pay attention to links in emails that you connect to. Try hovering over the link before you click it; you should see the destination URL at the bottom right of your browser.
    - Is the link familiar to you?
    - When you hover over the link, does the link match the display text for the link?
    - If not, do not click on the link.
- sense of urgency being created or a threat of loss to the service or facility being made from an email.
- requests for confidential information like password or pin number or bank details

- an email that looks authentic but has spelling or grammar mistakes that a professional organisation wouldn't make
- links to websites that have peculiar names or spelling
- free offers to iPads or holidays or other inducements
- be wary of the timing of emails sent at unusual hours e.g., 3.00am

**Purpose of use**

Bridge Mills Galway Language Centre require emails to be used solely for the purpose of your role within Bridge Mills Galway Language Centre.

**Do not use Bridge Mills Galway Language Centre emails to state your personal opinions**

Do not provide any unsolicited opinions about individuals which are outside the scope of your as an employee of Bridge Mills Galway Language Centre.

Bridge Mills Galway Language Centre emails may be accessed where necessary to form part of an enquiry internally or externally including but not limited to:

- Data Protection Acts
- Disciplinary
- Legal claim
- Incident or accident
- Auditors
- Regulators

Should any personal data relating to an individual (known as a data subject within GDPR) be included in emails, this will be provided to the relevant individual on receipt of a Data Subject Access Request.

**Sensitive Data**

Never send or forward sensitive data via email. Send sensitive data via the secure portals or password protected where the password is sent via text/SMS or send the file via SharePoint.

**Emails are monitored are part of the network security controls.**

Each employee should be aware that Bridge Mills Galway Language Centre will monitor all the organisation owned devices, communications and downloads that pass through its facilities to safeguard the network.

Should an investigation be required, Bridge Mills Galway Language Centre will first investigate other, less invasive means to protect the confidentiality of data and the security of the network. Any information retained on Bridge Mills Galway Language Centre facilities may be disclosed to the Gardai if a valid request is presented. If there is evidence that you are not adhering to the guidelines set out in this policy, Bridge Mills Galway Language Centre reserves the right to take disciplinary action up to and including dismissal and/or legal action.

If in exceptional circumstances, where authorised to use your Bridge Mills Galway Language Centre email for personal private use by your line manager, it is your duty to delete all personal emails (from all folders e.g., inbox, outbox) immediately after such communication. This to ensure your privacy is maintained where technically feasible.

**Who we are**

An English school providing quality tuition to its students. Data collection, processing, and use are conducted solely for the purpose of carrying out our role as an English school.

Bridge Mills Galway Language Centre's Employee's Data Protection Policy refers to our commitment to our compliance to data protection legislation including the Irish Data Protection Acts and the EU General Data Protection Regulation (GDPR).

Throughout this document "we", "us", "our", and "ours" refers to Bridge Mills Galway Language Centre

**How to contact us**

There are many ways you can contact us, including by phone, email, and post. More details can be seen here : https://www.galwaylanguage.com/contact-us/.

Our registered address is The Bridge Mills, Galway, H91 R1WF, Ireland

Contact Data Protection Lead: Patrick Creed
Telephone 091 566468

**Our role**

Bridge Mills Galway Language Centre processes personal data of all employees. Bridge Mills Galway Language Centre will process all such data in accordance data protection legislation including the Irish Data Protection Acts and the EU General Data Protection Regulation.

**Purpose for collecting your data**

The purposes for which we process the personal data on employees are:

- To manage the progression of each employee throughout their tenure of employment
- To ensure that correct training and development is provided
- To ensure employees are correctly rewarded for their service to the appropriate bank accounts
- To engage with Revenue for payment of employment taxation
- To manage the pension requirements of an employee until termination of pension
- To comply with all relevant law
- To ensure contact details of employees are available if required for the purpose of providing our services
- To manage the health, safety and security of our employees during employment
- To facilitate the prevention, detection and investigation of crime and the apprehension or prosecution of offenders
- To investigate, exercise or defend legal claims or other claims of a similar nature;

- To manage any disputes, should they arise
- To ensure a next of kin can be contacted if required
- To ensure all time, attendance and leave is recorded correctly
- To validate the employee is eligible for employment
- To safeguard the IT Network

Next of Kin

- To ensure a next of kin can be contacted if required

**Who we share your personal data with**

Your personal information may also be processed by other organisations on our behalf for the purposes outlined above. We **may** disclose your information where necessary to the following

- Agents, Host Families, Teachers, staff, interns, payroll, Revenue, Social Welfare. Data Protection Commission, outsourced Employment Law advisors, auditors, pension brokers & trustees, financial institutions, consultants, IT providers, couriers, shredding company, security company, printing company, accountant, insurers, partners, associates, agents or subcontractors, medical professionals and to possible successors to our business
- We may also disclose your information for the prevention and detection of crime and to protect the interests of the Bridge Mills Galway Language Centre or others, or if required to do so by law or other binding request.
- We may share your personal data with English Education Ireland for Garda vetting.

**Processing your information outside the EEA**

Some of third parties we share your data with may reside outside the European Economic Area (which currently comprises the Member states of the European Union plus Norway, Iceland and Liechtenstein). If we do this, your information will be treated to the same standards adopted in Ireland and include the following data protection transfer mechanisms:

- Model Clauses (also known as Standard Contractual Clauses) are standard clauses in our contracts with our service providers to ensure that any personal data leaving the EEA will be transferred in compliance with EU data-protection law. Copies of our current Model Clauses are available on request.
- Transfers to countries outside the EEA which have an adequate level of protection as approved by the European Commission (such as the United Kingdom).
- Transfers permitted in specific situations where a derogation applies as set out in Article 49 of the GDPR. For example, where it is necessary to transfer information to a non-EEA country to perform our contract with you.

**How we safeguard your personal data**

Bridge Mills Galway Language Centre ensures all employees personal data is processed subject to sufficient organisational and technical safeguards to protect employee data.

Bridge Mills Galway Language Centre collects this data in a transparent way and only with the full knowledge of interested parties. Once this information is available to Bridge Mills Galway Language Centre, the following rules apply. Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by Bridge Mills Galway Language Centre on the basis of either a valid contract, consent, legal compliance or legitimate interest
- Protected against any unauthorised or illegal processing by internal or external parties.

Our data will not be:

- Communicated to any unauthorised internal or external parties
- Stored for more than a specified amount of time.
- Transferred to organisations, states or countries outside the European Economic area without adequate safeguards being put in place as required under Data Protection law.

Bridge Mills Galway Language Centre's commitment to protect your data:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in data protection and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorisation etc.).

**What personal data we collect**

We collect and process your personal data in the course of business as an employee. This personal data includes any offline physical data or online data that makes a person identifiable.

We process data for the following groups of individuals (current and former)

A. Staff Members
B. Next of Kin

| **Types of Personal Data (i.e. any information relating to an identified or identifiable person)** | |
|---|---|
| **Demographic Data** | e.g. name, date of birth, age, |
| **Contact Details** | e.g. home/work landline phone number, personal/work mobile, home/work postal address, personal/work email address |

| | |
|---|---|
| **Financial Data** | e.g. bank account number, credit card number |
| **Digital Identifiers** | e.g. IP Address, MAC Address, X/Y Geographic Coordinate, meta data, cookie identifier, radio frequency identification (RFID) tags, advertising IDs, pixel tags, account handles, device fingerprints, browsing history |
| **Special Data** | e.g. data relating to racial or ethnic origin, political, religious or, philosophical beliefs, trade union membership, health, sexual life or orientation, genetic or biometric data. [note make it clear what is actually captured e.g. A assessment of the working capacity of the employee conducted by an independent medical professional where the statement of ability to work is provided to the us, Health data captured as part of an accident report, etc]. |
| **Criminal Offences/Convictions** | [e.g offences which impact on the ability to drive a company insured vehicle] Garda vetting results |
| **Government Identifiers** | driver's licence, income tax number |
| **Time Records** | Timesheets |
| **Health and Safety data** | As required |
| **Employment Progression** | Staff progression |
| **Disciplinary/investigations** | Reports of incidents/investigations |

**When do we collect sensitive personal data**

Sensitive data is known as special categories of data in Data Protection law. Special categories of data are defined by GDPR as processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

We will process special categories of personal data in the following circumstances:
1.In limited circumstances, with your explicit written consent.
2.Where we need to carry out our legal obligations such as Health and Safety and in line with our data protection policy.
3.Where it is needed in the public interest, and in line with our data protection policy
4 As your employer for the assessment of the working capacity of you as our employee where the assessment is conducted by a health professional.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

**When do we receive your data from a third party**

Where is it necessary, we may receive your data indirectly from the following sources:

- referees as provided by potential employees
- health professional as part of capacity to complete employment role
- Revenue and other Government Departments as part of the employee process
- Results from Garda vetting from the Marketing English Institute

**Consent options**

Where consent is relied upon as a basis for processing of any personal data, you will be presented with an option to agree or disagree with the collection, use or disclosure of personal data.

**What are the legal bases we process your data**

We collect your data based on the following legal basis

- Consent- where you have explicitly agreed to us processing your information for a specific reason such as explicit consent for us to process certain special categories of data about you;
- Contract-where you have entered into a contract of employment and are bound by providing personal data as required to fulfil the contract terms.
- Compliance -the processing is necessary for compliance with a legal obligation we have such as keeping records for revenue or tax purposes or providing information to a public body or law enforcement agency;. we may be required to process certain data to carry out our obligations under employment, social security or social protection law; the processing is necessary for the establishment, exercise or defence of legal claims
- Legitimate Interest Processing is necessary for the purposes of a legitimate interest pursued by us to safeguard the safety and security of human resources and our property. To provide our services to you as an employee of the company. To ensure that our IT network is safeguarded, to ensure that any complaints are managed effectively, to prevent fraud, report a potential crime, and to manage the progression of each employee throughout their tenure of employment
- Special categories of data, explicit consent as referred to above is only one lawful way to process health data, we may process your health data where it is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and

social security and social protection law or processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity or processing of health data may be collected where necessary and proportionate for the assessment of the working capacity of the employee conducted by a medical professional.

**What happens if you do not provide us with the data if legal basis is compliance or contract**

Where lawful basis is a contractual or statutory requirement, if an employee is obliged to provide the personal data, failure to provide this information may result in failure to retain a post.

**How long will we hold your personal data?**

We will only retain personal data for as long as necessary for the purposes for which it was collected; as required by law or regulatory guidance to which we are subject or to defence any legal actions.

**Disciplinary Consequences**

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

**Rights of the employee**

- You have the right of access to your personal data
- You have the right to rectification to any errors of your personal data
- You have the right to erasure of your personal data
- You have the right to restriction of processing
- You have the right to data portability
- You have the right to know if any automated decision's are made about you
- You have the right to object
- You have the right to compliant to the Data Protection Commission

**Rights Template and Rights policy**

**Right to Erasure**

**When have I the right to all my personal data being deleted by Bridge Mills Galway Language Centre?**

You have the right to have your personal data deleted without undue delay if:

- The personal data is no longer necessary in relation to the purpose(s) for which it was collected/processed
- You are withdrawing consent and where there is no other legal ground for the processing
- You object to the processing and there are no overriding legitimate grounds for the processing
- The personal data has been unlawfully processed
- The personal data must be erased so that we are in compliance with legal obligation
- The personal data has been collected in relation to the offer of information society services with a child.

**What happens if Bridge Mills Galway Language Centre has made my personal data public?**

If we have made your personal data public, we, taking account of available technology and the cost of implementation, will take reasonable steps, including technical measures, to inform those who are processing your personal data that you have requested the erasure.

**What happens if Bridge Mills Galway Language Centre has disclosed my personal data to third parties?**

Where we have disclosed your personal data in question to third parties, we will inform them of your request for erasure where possible. We will also confirm to you details of relevant third parties to whom the data has been disclosed where appropriate.

**Right to Data Portability**

**When can I receive my personal data in machine readable format from Bridge Mills Galway Language Centre?**

You have the right to receive your personal data, which you provided to the **Bridge Mills Galway Language Centre**, in a structured, commonly used and machine-readable format. You have the right to transmit this data to another organisation without hindrance from the **Bridge Mills Galway Language Centre** to which the personal data have been provided, where:

- processing is based on consent or contract
- processing is carried out by automated means.

**Would Bridge Mills Galway Language Centre transfer the personal data to another service provider if I requested this?**

We can transfer this data to another company selected by you on your written instruction where it is technically feasible taking account of the available technology and the feasible cost of transfer proportionate to the service we provide to you.

**Under what circumstances can Bridge Mills Galway Language Centre refuse?**

You will not be able to obtain, or have transferred in machine-readable format, your personal data if we are processing this data in the public interest or in the exercise of official authority vested in us.

**Will Bridge Mills Galway Language Centre provide me with my personal data if the file contains the personal data of others?**

We will only provide you with your personal data, ensuring we protect the rights and freedoms of others. Where personal data of another person may be on the same files as yours, we will redact the full details of the other person.

**Right for Automated Individual Decision Making including Profiling**

**What are my rights in respect of Automated Decision making?**

Bridge Mills Galway Language Centre does not have any automated decision-making processes. Where any such processes are introduced, we will provide you with the relevant information required under the "General Data Protection Regulation".

**Right to Object**

**Have I already been informed about my right to object?**

We have informed you of your right to object prior to us collecting any of your personal data as stated in this notice.

**When can I object to Bridge Mills Galway Language Centre processing my personal data?**

You can object on grounds relating to your situation, at any time to processing of personal data concerning you which is based on one of the following lawful basis

- public interest or
- legitimate interest,

including profiling based on those provisions.

Bridge Mills Galway Language Centre will stop processing your personal data unless:

- we can demonstrate compelling legitimate grounds for the processing, which override your interests, rights and freedoms
- the processing is for the establishment, exercise or defence of legal claims.

**What are my rights to object for direct marketing purposes?**

Where your personal data is processed for direct marketing purposes, you have the right to object at any time to processing of personal data concerning you for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where you object to processing for direct marketing purposes, we will no longer process this data for such purposes.

**What are my rights to object in the use of information society services?**
In the context of the use of information society services, you may exercise your right to object by automated means using technical specifications.

**Right to Restriction of Processing**

**When can I restrict processing?**
You may have processing of your personal data restricted:

- While we are verifying the accuracy of your personal data which you have contested
- If you choose restricted processing over erasure where processing is unlawful
- If we no longer need the personal data for its original purpose but are required to hold the personal data for defence of legal claims
- Where you have objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our legitimate grounds override.

**What if Bridge Mills Galway Language Centre has provided my personal data to third parties?**
Where we have disclosed your personal data in question to third parties, we will inform them about the restriction on the processing, unless it is impossible or involves disproportionate effort to do so.

**How will I know if the restriction is lifted by Bridge Mills Galway Language Centre and/or relevant third parties?**
We will inform on an individual basis when a restriction on processing has been lifted.

**Right of Rectification Policy**

**What can I do if Bridge Mills Galway Language Centre is holding incorrect personal data about me?**
Where you suspect that data we hold about you is inaccurate, we will on demand rectify any inaccuracies without undue delay and provide confirmation of same.

**What happens if Bridge Mills Galway Language Centre has disclosed my personal to third parties?**
Where we have disclosed inaccurate personal data to third parties, we will inform them and request confirmation that rectification has occurred. We will also provide you with details of the third parties to whom your personal data has been disclosed.

**VII Right to withdraw Consent**
**Under what circumstances could I withdraw consent?**
You can withdraw consent if we are processing your personal data based on your consent.

**When can I withdraw consent?**

You can withdraw consent at any time.

**If I withdraw consent what happens to my current data?**

Any processing based on your consent will cease upon the withdrawal of that consent. Your withdrawal will not affect any processing of personal data prior to your withdrawal of consent, or any processing which is not based on your consent.

**Right to lodge a complaint**

**Can I lodge a complaint with the Data Protection Commission?**

You can lodge a complaint with the Data Protection Commission in respect of any processing by or on behalf of Bridge Mills Galway Language Centre of personal data relating to you.

**How do I lodge a complaint?**

Making a complaint is simple and free. All you need to do is write to the Data Protection Commission giving details about the matter. You should clearly identify the organisation or individual you are complaining about. You should also outline the steps you have taken to have your concerns dealt with by the organisation, and what sort of response you received from them. Please also provide copies of any letters between you and the organisation, as well as supporting evidence/material.

**What happens after I make the complaint?**

The Data Protection Commission will then take the matter up with Bridge Mills Galway Language Centre on your behalf.

**Right of Access Policy**

**When do I have the right to access my personal data from Bridge Mills Galway Language Centre**

Where Bridge Mills Galway Language Centre process any personal data relating to you, you have the right to obtain confirmation of same from us, and to have access to your data.

**What information will Bridge Mills Galway Language Centre provide to me?**

If we are processing your personal data, you are entitled to access a copy of all such personal data processed by us subject to a verification process to ensure we are communicating with the correct person. We will provide any of the following information:

- why we are processing your personal data
- the types of personal data concerned
- the third parties or categories of third parties to whom the personal data have been or will be disclosed. We will information you if any of the third parties are outside the European Economic Area (EEA)or international organisations
- how your personal data is safeguarded where we provide your personal data outside the European Economic Area or to an international organisation

- the length of time we will hold your data or if not possible, the criteria used to determine that period
- your rights to:
    - request any changes to inaccurate personal data held by us
    - have your personal data deleted on all our systems
    - restriction of processing of personal data concerning you
    - to object to such processing
    - data portability
- your right to lodge a complaint with the Data Protection Commission info@dataprotection.ie
- where we have collected your personal data from a third party, we will provide you with the information as to our source of your personal data
- any automated decision-making, including profiling which includes your personal data. We will provide you with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for you.

**What Information Is not provided**

- Business Information pertaining to your role as an employee
- If we do not provide you with your personal data, we have an obligation to give reasons why this personal data is being withheld.

**How long will it take to receive my personal data from Bridge Mills Galway Language Centre?**

We will provide you with a copy of the personal data we are currently processing within one month of request. In rare situations if we are unable to provide you with the data within one month we will notify you, within one month, explaining the reason for the delay and will commit to delivery within a further two months.

**How much will it cost me to receive my personal data?**

We will not charge for providing your personal data unless we believe the request is excessive and the cost of providing your data is disproportionate to your services provided.

**Can I request additional copies of my personal data?**

If you require additional copies we will charge €20 to cover our administrative costs.

**Can I receive my personal data electronically?**

You can request your personal data by electronic means and we will provide your personal data in a commonly used electronic form if technically feasible.

**What will Bridge Mills Galway Language Centre do if another person's personal data is shared with my personal data?**

We will only provide you with your personal data, ensuring we protect the rights and freedoms of others.  Where personal data of another person may be on the same files as yours, we will redact the full details of the other person.

# Who we are

Bridge Mills Galway Language Centre's Privacy Statement refers (together with our Cookies Policy [see appendix 2]) to our commitment to our compliance to data protection legislation including the Irish Data Protection Acts and the EU General Data Protection Regulation.

Throughout this document "we", "us", "our", and "ours" refers to Bridge Mills Galway Language Centre.

# How to contact us

There are many ways you can contact us, including by phone, email, and post. More details can be seen here https://www.galwaylanguage.com/.

Our registered address is: The Bridge Mills, Galway, H91 R1WF, Ireland.
Contact Data Protection Lead: Patrick Creed director@galwaylanguage.com
Telephone: +353 91 566 468.

# What happens if we make changes to this notice

Where changes to this Privacy Statement occur, the updated version will be published on our website and where appropriate/possible communicated directly to individuals through a communication channel such as email and/or our social media.

Current version Reference [V1.01 23/01/2025]

# Who do we collect data about

We collect and process your personal data only when such data is necessary in the course of providing our English Language services to you. This personal data includes any offline physical data or online data that makes a person identifiable.

We process data for the following groups of individuals where it is necessary:

A. Students

B. Guardians
C. Teachers
D. Educational Partners
E. Host Families
F. Potential candidates for employment
G. Contractors and Suppliers
H. Next of Kin

We are the controller for the personal information we process, unless otherwise stated.

# What types of your data do we collect

You directly provide us with most of the data we collect. We collect data and process data when you:

- Apply and attend one of our courses
- Provide a service to our school
- Provide accommodation to our students
- Voluntarily complete a survey or provide feedback
- Use or view our website via your browser's cookies
-

As part of our services to you, we ***may*** need to obtain and process personal data as required ***where necessary*** to provide our services such as:

## Students' information collected

Your name, address, Eircode (Postal code), phone number [landline & mobile], email, date of birth (or age), signatures, proof a eligible visa if required, Photo ID, attendance records, course progress and results, interactions with our teachers and staff recorded, by phone, or email, current or past complaints, occupation, cookie consent and marketing consent, relevant medical history if provided, Health and Safely reporting if required.

## Guardians

Parent/Guardian-Name, address, email, signature, phone number, proof of ID, consent- authorisation form with relevant medical history if provided.

## Teachers [this is for teachers not employed full time]

Name, Address, Next of Kin name, Next of Kin contact number, signatures, , Photo ID,Passport Details, PPSN, Marital Status, Date of birth, Email Address, Mobile Number, Landline, Bank Account details-IBAN, BIC, Brief statement of duties, Start Date, Hours of work, CV, Work Permit Details, Increment Date, Salary, Allowances, Qualifications,

Annual Leave, Entitlement, Garda Vetting Results, Proof of work, Contract of employment, Poof of ID, Training Records, Lateness records, Temporary shortage of work, Time sheets, Payroll details, Occupation, Job Classification, Payment records, Pension records, Taxation records P60/s etc, Allegations and complaints, Minutes of meetings, Performance records, Probationary records, Maternity Leave details, Parental Leave details, Force Majeure leave, Career's Leave, Bereavement leave, Travel expenses, Grievance documentation, Health & Safety documentation, Alcohol & Drugs documentation, Disciplinary, Sickness or injury recorded at work, Notification of incapacity for work, Annual/sick leave records, Medical Certs, Medical health data, Return to work documentation, Photos. Current or past complaints
IT safeguard monitoring activities- location/transactional/ time log, video recordings, digital photos, Health and Safely reporting if required.

## Educational Partners

Your name and business contact details (work- address, email, phone), Signatures, Health and Safely reporting if required.

## Host Families

Your name, address, Eircode (Postal code), phone number [landline & mobile], email, signatures, students hosted records, garda vetting records (Proof of identification e.g. Passport or Driving Licence, Proof of address,) current or past complaints, financial payments records.

## Potential candidates for employment

Your name and contact details (i.e. address, home and mobile phone numbers, email address), CV, and covering letter, Interview assessment details, Any information you provide to us by email, telephone or during an interview, Details of your referees.

## Contractors and Suppliers

Your name (and your employees names when required) and business contact details (work- address, email, phone (and your employees names when required)),Brief statement of duties, Job classification, Start date and contracted price, Registered Directors details as publicly available on the Company's registration Office, Signatures, Details of your referees, Health and Safely reporting if required, Due Diligence compete of supplier pre commencement of services.

## Next of Kin

Name, Relationship, Telephone, email

# When do we collect sensitive personal data

Sensitive data is known as special categories of data in Data Protection law. Special categories of data are defined by GDPR as processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. We may collect the following special categories of data where necessary:

- Medical information provided by you which you feel is necessary for the school to know in the event of an emergency
- Religious beliefs provided by you which you feel is necessary for the school to know
- Natural person's sex life or sexual orientation which you feel is necessary for the school to know

We will process special categories of personal data only with your explicit written consent unless we need to carry out our legal obligations and in line with our data protection policy or less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

# When do we receive your data from a third party

Where is it necessary for the service provided, we may receive your data indirectly from the following sources:

- Student may provide your information as their next of kin
- Appointed Referees provided by you
- Professional Bodies as proof of qualifications
- Education providers as proof of qualifications
- National Vetting Bureau will provide English Education in Ireland with the vetting disclosure for the schools and host family. The individual school will receive the relevant disclosure for their applicants only.
- Education agents, and Partners

# What are the legal bases we process your data

We collect your data based on the following legal basis:

## Consent

Where you have explicitly agreed to us processing your information for a specific reason such as

- Marketing (see section 14)
- Any individual
    - Photograph or videos for publication at events
- Cookie (see cookie policy)
- Parental Consent
  If you're 16 or 17 State, your parent or guardian needs to provide consent for us to use your information.

## Right to withdraw consent at any time

Where consent is relied upon as a basis for processing of any personal data, you will be presented with an option to agree or disagree with the collection, use or disclosure of personal data. Once consent is obtained, it can be withdrawn at any stage.

## Contract

Processing is necessary for the performance of a contract with you or in order to take steps at your request prior to entering into a contract.

## Compliance

The processing is necessary for compliance with a legal obligation we have such as keeping records for revenue or tax purposes or providing information to a public body or law enforcement agency; we may be required to process certain data to carry out our obligations under social security or social protection law. We may also disclose your information if required to do so by law. We are required by law to process that data in order to ensure we meet our national legislative requirements.

Where it is necessary and proportionate, we may allow authorised people to see our records (which may include information about you) for reporting, compliance and auditing purposes.

### Legitimate interest

Processing is necessary for the purposes of a legitimate interest pursued by us to safeguard the safety and security of our employees, teachers, property, and students, IT systems and devices, buildings, information located or stored on the premises, and assets, and those of service providers, consultants, and advisors that assist us in carrying out its functions. The processing is necessary for the establishment, exercise or defence of legal claims. We may also disclose your information for the prevention and detection of crime and to protect the interests of us or others. To inform recruitment decisions taken about appointments and new hires. To operate our business generally and manage and administer our services to students, teachers, suppliers and potential candidates and provide surveys (see Section 15).

# What happens if you do not provide us with the data if legal basis is consent or contract

Where lawful basis is a statutory or contractual requirement, if you are obliged to provide the personal data, failure to provide this information may result in us being unable to provide our services to you or obtain your services.

# What is the purpose (s) for processing your data

We process your data to provide this service.

You agree that any data you provide to us will be true, complete, and accurate in all respects and you agree to notify us immediately of any changes to it. We will only collect personal information from or about you which is necessary for the following purposes:

General

- To provide this website to you and respond to your queries
- To comply with all relevant law
- To manage your safety and security while you are on our premises
- To facilitate the prevention, detection and investigation of crime and the apprehension or prosecution of offenders
- To investigate, exercise or defend legal claims or other claims of a similar nature.

## Students

- To provide quality tuition to you
- Set up and administer your account as a student with us
- To maintain our relationship with you whilst you are a student and investigate any complaints or disputes or accidents
- Contact you for direct marketing purposes, subject to restrictions under the relevant laws, including the right to opt out of such marketing
- Provide you with information relating to our services
- Provide you with progression of your course and results of any assessments
- To provide essential communication with you, including to respond to information requests submitted
- To obtain your feedback on our tuition services
- To notify you about changes to contracted services relevant to you

## Guardians

- To provide the services to the minor and communicate with you all relevant information for the purposes as listed under section 10A above under Students
- To contact you in the case of an emergency of the minor
- To only process the minor's personal data where you have consented for us to do so

## Teachers

- To complete our due diligences on your application before offering a position
- To offer teaching services at our school
- To capture the progress of your services to our students
- To ensure you provide qualify tuition to our students

## Educational Partners

- To offer other services at our school

## Host Families

- To find suitable Host Families
- To find suitable accommodation for our students

## Potential candidates for employment

- To assess the applicants
- Identify suitable candidates for the posts
- Interview the candidates

## Contractors and Suppliers

Set up, avail of your services, contact you and administer our account as a customer with you

## Next of Kin

To ensure a next of kin can be contacted if required

# What you need to do when you provide us with other individuals information data

If you are providing personal information on behalf of a third party, you must ensure that the third party receives a copy of this Privacy Statement before their personal information is shared with us (e.g., Next of Kin, References, etc).

You do not need to provide this Privacy Statement in the following situations

- the individual already has the information
- obtaining or disclosure such information is expressly laid down in the law to which the school must comply and which provides appropriate measures to protect the individual's legitimate interests
- where the personal data must remain confidential subject to an obligation of professional secrecy regulated by law.

# How we protect your data

We collect this data in a transparent way and only with the full knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up to date
- Collected fairly and for lawful purposes only
- Processed by us based on either a valid contract, consent, legal compliance or legitimate interest
- Protected against any unauthorised access or illegal processing by internal or external parties.

Our data will not be:

- Communicated to any unauthorised internal or external parties
- Stored for longer than required for the purpose obtained
- Transferred to organisations, states, or countries outside the European Economic Area without adequate safeguards being put in place as required under Data Protection Law.

Our commitment to protect your data:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in data protection and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse

- Establish data protection practices (e.g., document shredding, secure locks, data encryption, frequent backups, access authorisation etc.).

## How our third-party providers protect your data

We only engage with third-party service providers who provide sufficient guarantees to protect your data following our instructions and are bound by a data processing agreement.

## How we use your information as a member for Marketing

As part of improving our service to you, from time to time, we would like to inform you of services, and/or promotional offers available from us. We may wish to use different means when sending such marketing communications.

We can reach out to you with this information in all sorts of ways:

- by e-mail
- post
- telephone

We may share your data with third parties' software and marketing providers so that they may send you messaging on our behalf.

Opt in
Where you have consented to marketing by opting in to marketing, we will send you marketing.

You have a right to notify us free of charge at any time that you wish to refuse such marketing by writing to us at our address at the top of this document or by using the "opt-out" options in any marketing message we send you.

## How we use your information for Surveys

We would like the opportunity to understand your experiences with us and to monitor the performance and effectiveness of our delivery of services to you. We would like to assess the quality of our member services. We promise to listen to our students and to adapt to the recommendations provided to ensure our students are receiving the best quality service from us. From time to time, we may conduct student satisfaction surveys.

Where we do so, we rely on the lawful processing of legitimate interest to enhance our service delivery. A withdrawal option will be provided in all survey communication thereafter.

# Who we share your information with

Your personal information may also be processed by other organisations on our behalf for the purposes outlined above. We **may** disclose your information ***where necessary*** to the following

Employees, Teachers, Educational Partners, Host Families, Revenue, Social Welfare. Data Protection Commission, legal advisors, business advisors, financial and leasing institutions, law enforcement, debt collectors, IT providers, couriers, shredding company, security company, printing company, CCTV company, administration services, accountant/auditors, insurers, recruitment agents, marketing consultants or subcontractors and to possible successors to our business.

# How long will we hold your information

We will only retain personal data for as long as necessary for the purposes for which it was collected as required by law or regulatory guidance to which we are subject or to defend any legal actions.

# Unsolicited and Solicited CV's

## Using email to communicate

Any information you send to Bridge Mills Galway Language Centre via email is sent via an unsecured email link. Due to the nature of the Internet, there is a possibility that unsecured (unencrypted) email could be intercepted and read by third parties. Bridge Mills Galway Language Centre assumes no responsibility for interception of confidential information (including in a CV) that you send in an unsecured (unencrypted) email message.

## Right to Hire

Any employment agency, person or entity that submits an unsolicited Curriculum Vitae (CV) to Bridge Mills Galway Language Centre does so with the understanding that Bridge Mills Galway Language Centre will have the right to hire that applicant at its discretion without any fee owed to the submitting employment agency, person or entity.

## Application for an unsolicited job

If you are interested in applying for an unsolicited job within Bridge Mills Galway Language Centre you may provide us with your CV. We will then match your qualifications and experience to the position you applied for, or any other current job opportunity. If your profile corresponds to our requirements, we will contact you.

**Application for a solicited job**

If you are interested in applying for a solicited job within Bridge Mills Galway Language Centre you may provide us with your CV. We will then match your qualifications and experience to the position you applied for, or any other current job opportunity. If your profile corresponds to our requirements, we will contact you.

**Verification**

Verification checks are required for specific roles and will be identified in the job advertisement where relevant. Verification checks such as:

- Reference checks
- Proof of Identity
- Proof of Residency
- Proof of the Right to Work
- Garda Vetting (only in limited circumstances)
- Background checks (state clearly what will be conducted e.g.)
    - verifying qualifications with educational establishments
    - checking medical history for working capacity of the employee for the relevant job
    - checking professional social media profiles

Upon commencement of contract, we may process the following data depending on specific roles.

- Biometrics

## Deletion and rectification of your personal data

Personal data processed because of unsolicited job applications, where the job applicant is not offered a job, will be deleted after the rejection of application has been sent to the job applicant, unless the job applicant accepts the storage for a longer period.

## Sensitive personal data

Bridge Mills Galway Language Centre endeavours not to collect "sensitive personal data" via CV's. By "sensitive personal data" is meant personal data relating to race or ethnic origin, political opinions, religious or philosophical beliefs, membership of trade unions, or health or sex life. If you make unsolicited sensitive personal data available to us (for example, by

including this on a C.V.), you are required to provide explicit consent for Bridge Mills Galway Language Centre to process this data.

Please do not provide your date of birth, your age or your PPS number on your CV.

## Processing your information outside the EEA

Some third parties we share your data with may reside outside the European Economic Area (which currently comprises the Member states of the European Union plus Norway, Iceland and Liechtenstein). If we do this, your information will be treated to the same standards adopted in Ireland and include the following data protection transfer mechanisms:

- Model Clauses (also known as Standard Contractual Clauses) are standard clauses in our contracts with our service providers to ensure that any personal data leaving the EEA will be transferred in compliance with EU data-protection law. Copies of our current Model Clauses are available on request.
- Transfers to countries outside the EEA which have an adequate level of protection as approved by the European Commission (such as the United Kingdom).
- Transfers permitted in specific situations where a derogation applies as set out in Article 49 of the GDPR. For example, where it is necessary to transfer information to a non-EEA country to perform our contract with you.

## How to exercise your information rights

- You have the right of access to your personal data
- You have the right to rectification to any errors of your personal data
- You have the right to erasure of your personal data
- You have the right to restriction of processing
- You have the right to data portability
- You have the right to know if any automated decisions are made about you
- You have the right to object
- You have the right to compliant to the Data Protection Commission

# TEMPLATES

## **TEMPLATE**: Bridge Mills Galway Language Cente Contract Insert for Data Controller for a School Version 1.02

Insert for both the Educational Partners (agents) and Host Families. Also for any other third party acting as an independent Data Controller

*Both parties shall act in their capacity as Data Controllers in relation to Personal Data shared between the parties in the course of the provision of the Services.*

[Educational Partners or Host Families-insert relevant name] *will ensure that:*

*adequate privacy notices have been provided to its students and their guardians [state others if not included]whose data will be collected through use of the Services so they understand the circumstances their Personal Data will be shared with Bridge Mills Galway Language Centre and the purpose of the sharing;*

*it has a lawful basis for processing the Personal Data which allows* [Educational Partners or Host Families-insert relevant name] *to share the Personal Data with Bridge Mills Galway Language Centre and for Bridge Mills Galway Language Centre to use any Personal Data in the course of providing Services; and*

[Educational Partners or Host Families-insert relevant name] *shall endure its students and their guardians [state others if not included]are informed on how to access Bridge Mills Galway Language Centre privacy policy which is available on Bridge Mills Galway Language Centre website or by contacting your Account Manager if a hard copy is required.*

*19.3 Where* [Educational Partners or Host Families-insert relevant name] *provides Personal Data to Bridge Mills Galway Language Centre, the data is transferred on a controller-to-controller basis. The transfer of personal data from Bridge Mills Galway Language Centre to* [Educational Partners or Host Families-insert relevant name] *is likewise transferred on a controller-to-controller basis.*

*The Parties agree to comply with all applicable Data Protection Legislation in relation to the processing of any Personal Data in connection with the provision of the services.*

*In the event its students and their guardians [state others if not included] seeks to exercise their rights as a Data Subject each party shall have a contact point for the fulfilment of Data Subject rights and be responsible for fulfilment of same.*

*The terms 'processing', 'Personal Data', 'Data Processor' and 'Data Controller' shall be as defined in the Data Protection Legislation. The term 'Data Protection Legislation' shall mean the General Data Protection Regulation (EU) 2016/679, the Data Protection Acts 1988 to 2018, all as amended, modified, consolidated or re-enacted from time to time and all applicable national implementing legislation and guidelines, in each case, as amended, revised or replaced from time to time.*

**TEMPLATE**: Contract Insert for Data Processor 1.01

## Processor Agreement Clause Template

*This is a template processing clause. Every contract agreement is different, and this template may not be appropriate to the processing relationship between your organisation and your individual Clients/Customers. You should obtain independent legal advice prior to entering into any contract.*

**DATA PROCESSING AGREEMENT**

This Data Processing Agreement (**"Agreement"**) is made [date] (**"Effective Date"**)

**BETWEEN:**

**(1) The Data Controller provide full name, addressed and registered number and**

**(2) The Data Processor provide full name, addressed and registered number**

**(Together the "Parties" and a "Party" shall be construed accordingly).**

**AGREEMENT**

1. DEFINITIONS

Capitalised words and expressions used in this Agreement but not defined herein shall have the meanings given to such words and expressions in Regulation (EU) 2016/679 all as amended, modified, consolidated, or re-enacted from time to time (together, the "**Data Protection Legislation**").

1.1

In discharging its obligations under this Agreement, in so far as entity acts as a Processor, it is responsible for its compliance with all applicable data protection or privacy legislation and will ensure that all necessary registrations and notifications are made and provide the other, in its capacity as Controller with a copy, on request, of evidence of such and evidence of any amendments or alterations made thereto.

a. In respect of any personal data that Processor processes in the course of providing the services herein to Controller, Processor shall act as a data processor or sub-processor on Controller's behalf.

b. Processor shall only process personal data under the contract in accordance with the reasonable written instructions provided from the Controller and the written instructions, as stated in Schedule 1 and in accordance with applicable Data Protection Legislation, including in particular:

1.2.1 the adoption of appropriate Technical and Organisational Measures against accidental disclosure, loss or destruction of personal data as stated in Schedule 1
1.2.2 informing Controller within 24 hours in the event of unauthorised disclosure, loss or destruction of any personal data processed under this contract ("Security Incident") which comes to Processor's attention. Unless required by law or other obligation, Processor agrees that it will not communicate with any third party including but not limited to the media, vendors, consumers and affected individuals regarding any Security Incident without the consent and direction of Controller;
1.2.3 referring to Controller any requests, notices or other communication from Data Subjects, any Supervisory Authority or other law enforcement agency relating to personal data for Controller to resolve;
1.2.4 ensuring that Processor personnel processing personal data under the contract are under an obligation of Confidentiality; and
1.2.5 making available such reasonable information necessary to demonstrate compliance with this clause 1, including facilitation and assistance with audits and inspections whether conducted by Controller or another auditor mandated by Controller.

1.3 Where requested to do so in writing, and at the cost of Controller, Processor will make available such information and assistance as are reasonably necessary to Controller to comply with its obligations to

i. respond to requests for exercising the Data Subject's Rights
ii. report personal Data Breaches and
iii. conduct Data Protection Impact Assessments and Prior Consultation with Data Protection Authorities.

1.4 Controller acknowledges that Processor shall transfer personal data to third party sub-contractors (including group companies) to whom disclosure is reasonably

necessary in order for Processor to carry out the services herein and hereby provides its general authorisation [or prior specific authorisiation-Controller to decide] to such transfers, which will occur only where Processor has entered into a written agreement with each sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of your data to the extent applicable to the nature of the services provided by such sub-processor. Where a sub processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the Controller for the performance of that other processor's obligations. Processor shall inform Controller of any intended changes concerning the addition or replacement of other processors, thereby giving Controller the opportunity to object to such changes. Controller further agrees that Processor shall transfer personal data disclosed pursuant to the contract to such sub-contractors based outside the European Economic Area but only where adequate safeguards are put in place by Processor or such sub-contractors to protect such personal data as required under Data Protection Legislation and prior authorisation from the Controller.

1.5 Without prejudice to any other provision of this contract relating to termination, on termination of this contract, Processor shall, on written instructions from Controller, either delete or return all personal data processed as part of the contract to Controller unless Processor is subject to an overriding legal, regulatory or other requirement to retain such personal data.

_____
Name:
Title:
For and on behalf of Controller

_____
Date

_____
Name:
Title:

For and on behalf of Processor

_____

Date

## GDPR UPDATES 2025

1. BMGLC Clear Desk Policy v 1.**01**
2. Contract Insert for Data Controller for a School Version 1.02
3. Contract Insert for Data Processor 1.01
4. Bridge Mills Galway Language Centre Data Breach Policy Version 1.01
5. Bridge Mills Galway Language Centre Data Protection Governance Framework-Draft V1.01
6. Bridge Mills Galway Language Centre Garda Vetting Policy -Draft V1.00
7. Bridge Mills Galway Language Centre Company System Policy Version 1.01
8. Bridge Mills Galway Language Centre Insert for E-Mail Signature Version 1.01
9. Bridge Mills Galway Language Centre Joiners, Mover, leavers Policy Version 1.01
10. Bridge Mills Galway Language Centre **Email Policy** Version 1.00
11. Bridge Mills Galway Language Centre Employee Data Protection Policy Version 1.01
12. Bridge Mills Galway Language Centre Privacy Statement Version 1.0