Data Protection Policy

Introduction
Celtic English Academy needs to gather and use certain information about individuals. This can include students, suppliers, business contacts, employees, and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored in order to meet the company's data protection standards – and to comply with the law.

Why this policy exists
This data protection policy ensures that Celtic English Academy:

- complies with data protection law and follows good practice
- protects the rights of staff, customers and partners
- is open about how it stores and processes individuals' data
- protects itself from the risks of a data breach

This policy should be read alongside Celtic English Academy's Employee Handbook where data protection information is outlined in 'Section 2' and 'Section 13'.

Data Protection Law
The Data Protection Act 1998 describes how organisations – including Celtic English Academy – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. They say that personal data must:

1. be processed fairly and lawfully
2. be obtained only for specific, lawful purposes
3. be adequate, relevant and not excessive
4. be accurate and kept up to date
5. not be held for any longer than necessary
6. processed in accordance with the rights of data subjects
7. be protected in appropriate ways
8. not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, Risks and Responsibilities
Policy Scope
This policy applies to:

- all staff and volunteers of Celtic English Academy
- all students who have attended or are currently attending courses at Celtic English Academy
- all contractors, suppliers, and other people working on behalf of Celtic English Academy
- all buildings rented or owned by Celtic English Academy

It applies to all personal data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998.

This can include:

- names of individuals
- postal addresses
- email addresses
- telephone numbers
- any other information relating to individuals

Data Protection Risks

This policy helps protect Celtic English Academy from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them. A consent form will be given at the time of employment.
- Reputational damage. For instance, the company could suffer if anyone successfully gained access illegally to sensitive data.

Responsibilities

Everyone who works for or with Celtic English Academy has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The Directors are ultimately responsible for ensuring Celtic English Academy meets its legal obligations.

- The Organisational Development and Communications Manager is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies on an annual basis.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Celtic English Academy holds on them (also called ‘subject access requests’).
    - Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing (i.e. Google Drive) and student management (i.e. Fidelo) services.

- An outsourced GDPR representative, Gallery Teachers, is responsible for:
    - acting as a direct contact to the authorities and data subjects (Users/Customers)

- An outsourced IT Service, Carabiner IT Ltd, is responsible for:
    - Performing regular checks and scans to ensure security hardware and software is functioning properly, including anti-virus and malware software.

  - Maintaining networking equipment including all firewalls and routers.
  - Providing a general IT service to all staff (i.e. answering questions related to Data Protection, supporting them when IT issues arise, fixing machines as needed and so on).

- The Chief Executive Officer, Shoko Doherty, is responsible for:
  - Approving any data protection statements attached to communications, such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing (i.e. Google Drive) and student management (i.e. Fidelo) services.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Celtic English Academy will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used, and they must never be shared unless requested, for a specific purpose, by one of the Directors or by a line manager. For instance, hot-desking in the Academic Office may mean that teachers need to share their passwords with managers.
- Personal data should not be disclosed to unauthorised people, either within the company or externally. See the Identity Verification Procedure document.
- Data should be reviewed every 6 months and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of securely. As a rule, no data should be kept for more than 5 years without a valid reason. See the Records Retention Schedule document.
- Employees should request help from their line manager or the Organisational Development and Communications Manager if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT management company.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. For instance, HR files must be kept in a locked drawer/cabinet so that no unauthorised member of staff can gain access.

These guidelines also apply to data that is usually stored electronically, but has been printed out for some reason:

- If a paper file exists and it does not have an electronic copy which will be needed at a future point, it must be kept in a locked drawer or filing cabinet. Please refer to the Records Retention Schedule document.
- Employees should make sure that printouts or originals are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on destined drives and servers, and should only be uploaded to an approved cloud computing service.
- If used, servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones. This should be saved on the secured cloud computing system or via the Google Drive Shortcut.
- All servers and computers containing data should be protected by approved security software and a firewall IT (company to confirm).

Data Use
Personal data is of no value to Celtic English Academy unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should not be shared verbally (i.e. reading out debit card information over the phone in the presence of other staff), as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT company can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their computers. Always access and update the central copy of any data.

Data Accuracy
The law requires Celtic English Academy to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Celtic English Academy should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any duplicate data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call. Please see the Identification Verification Procedure.
- Celtic English Academy will regularly audit the information it holds on our data subjects and encourage them to maintain the accuracy of that data. For instance, the FrontDesk app allows students to update their personal information via their mobile device.
- Data should be updated as inaccuracies are discovered by the relevant staff member. For instance, if a student can no longer be reached by their stored telephone number it should be removed from the database by the staff member who discovered it.
- It is the Marketing Manager's responsibility to ensure marketing databases are checked against industry suppression files every 6 months.

Subject Access Requests
All individuals who are the subject of personal data held by Celtic English Academy are entitled to:

- ask what information the company holds about them and why.
- ask how to gain access to it.
- be informed how to keep it up to date.
- be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a 'Subject Access Request'.

Subject Access Requests from individuals should be addressed to the Organisational Development and Communications Manager by email. The Organisational Development and Communications Manager will then reply by sending the 'Subject Access Request' form to be completed by the individual making the request.

Individuals will be charged £10 per subject access request. The Organisational Development and Communications Manager will respond to the request within 40 days.

After receiving a subject access request, the Organisational Development and Communications Manager will always:

- verify the identity of anyone making a Subject Access Request (SAR) before handing over any information
- collect the £10 fee for the SAR
- ask for additional information that can help them fulfil the request
- note the name of the requester, date of the request and any steps taken on the 'Subject Access Request' spreadsheet
- reply to the request within the 40-day time limit

Disclosing Data for Other Reasons
In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Celtic English Academy, will disclose requested data. However, the Organisational Development and Communications Manager will ensure the request is legitimate and doesn't impinge on the rights of others. They are entitled to seek assistance from the board and form the company's legal advisers, where necessary.

Please refer to the Staff Data Protection and Student Data Protection Notices for specifics.

Providing Information
Celtic English Academy aims to ensure that individuals are aware that their personal data is used by the company.

In the case of mandatory inspections of Celtic English Academy carried out by Accreditation UK - British Council every effort will be made to remove student and staff personal data across documentation, as relevant, to ensure personal data is not disclosed e.g. removal of names and full addresses on accommodation lists, or login information on staff induction paperwork.

In the case of evidencing files with sensitive personal data, for example HR staff digital records, staff qualification lists and contracts, these will always be provided in the presence of Senior Management and limited to the confidential viewing of the inspecting persons only, for the purpose of meeting the inspection criteria. No copies will be made or shared.

[A version of this statement will also be made available on the company's website.]