etb

Bord Oideachais agus Oiliúna
Chill Chainnigh agus Cheatharlach
Kilkenny and Carlow
Education and Training Board

Data Protection
is YOUR Responsibility

Guide for KCETB Staff

June 2018

Message from the Chief Executive

Dear Colleagues

We are all aware that new European regulations about data protection came into effect in May 2018. Along with existing legislation, the new regulations ensure that people have specific legal rights to seek access to their personal information held by public organisations and private companies.

KCETB is committed to complying with the requirements of the legislation: to ensure that personal records and information are kept accurate and up-to-date, are kept safe and secure and are provided to people when they request them.

The purpose of this document is to summarise guidance for KCETB staff about their responsibilities under data protection legislation and regulations. It sets out the standards that all KCETB staff must apply to ensure that the personal information of students, parents/guardians and staff is used appropriately.

Data protection is everyone's responsibility. I hope this guide will assist you as a member of KCETB staff to understand what is required of you under data protection legislation. When you have read the guide, please follow the steps below, to fulfil your obligations under the legislation.

What to do next

1. **Each KCETB staff member must log on to the ETBI online training tool for GDPR at https://www.etbi.ie/?s=gdpr, registering your KCETB email address. You must then complete the GDPR Test to be GDPR compliant. A confirmation email will be sent to KCETB Corporate Services to confirm that staff members have completed the online test.**

2. **Please sign and return the "Confirmation Form" at the back of this document and return to your line manager.**

Thank you for your co-operation in this important matter.

Cynthia Deane
Chief Executive

Data Protection is YOUR Responsibility

In the course of their work, KCETB staff are required to collect and use certain types of information about people, including 'personal data' as defined by the Data Protection Acts. This information can relate to current, past and prospective students, employees, suppliers and others with whom staff communicate. In addition, staff may occasionally be required to collect and use certain types of personal information to comply with the requirements of legislation. KCETB collects and processes personal data in multiple formats every day. KCETB has a responsibility to ensure that this personal data is:

- obtained fairly
- recorded correctly, kept accurate and up-to-date
- used and shared both appropriately and legally
- stored securely
- not disclosed to unauthorised third parties
- disposed of appropriately when no longer required.

All staff working in KCETB are legally required under the Data Protection Acts 1988, 2003 and 2018 to ensure the security and confidentiality of all personal data they collect and process on behalf of students, employees and others. Data Protection rights apply whether the personal data is held in electronic format or in a manual or paper-based form. Staff breaches of data protection legislation may result in disciplinary action.

What is confidential personal data?

Any record containing personal identifiable information such as name, address, date of birth, PPS Number, employee number, or medical record is deemed confidential. Examples of confidential documents include personnel files, contracts, financial records, payroll records, legal documents or medical records.

Take These Practical Steps to Protect Data and Privacy

Personal information should not be deliberately or inadvertently viewed by uninvolved parties.

- Staff should operate a clear desk policy at the end of each working day and when away from the desk or the office for short or long periods.

- Personal and sensitive records held on paper and/or on screens must be kept hidden from callers to offices/ public hatches/staff rooms, etc.

- Records (student/employee files) containing personal information must never be left unattended where they are visible or maybe accessed by unauthorised staff or members of the public.

- If computers or VDUs are left unattended, staff must ensure that no personal information may be observed or accessed by unauthorised staff or members of the public.

- The use of secured screen savers is advised to reduce the chance of casual observation.

- Rooms, cabinets or drawers in which personal records are stored should be locked when unattended. A record tracing system should be maintained of files removed and/or returned.

- It is important to ensure that student or staff information is not discussed in inappropriate areas where it is likely to be overheard, including conversations and telephone calls. Particular care should be taken in areas where the public have access.

- While appreciating the need for information to be accessible, staff must ensure that personal records are not left on desks or workstations at times when unauthorised access might take place.

- Staff must only access personal information on a need to know basis and should only view or share data that is relevant or necessary for them to carry out their duties.

- Teachers/Tutors must not call out exam results/class test results in the classroom

- Teachers/Tutors must not project personal data belonging to anybody else onto a board/screen

- Teachers/Tutors Diaries: If student/learner/staff personal data are being entered in a teacher/tutor diary, the diary and its contents will be requested by KCETB if we receive a Freedom of Information (FOI) or Data Protection Request from a student or a parent/guardian. This applies irrespective of who provides and pays for the diary. Such diaries should be stored by the school/centre administration in accordance with the KCETB records management policy.

Do not leave information/data unattended in cars

- Staff must not leave laptops/portable electronic devices and/or files containing personal information unattended in cars.

- In cases where staff remove files/records from offices to attend meetings, home visits, etc. the records should always be contained in a suitable brief case/bag to avoid any inappropriate viewing and also to secure the records.

- All files and portable equipment must be stored securely. If files containing personal information must be transported in a car, they should be locked securely in the boot for the minimum period necessary.

- Staff should not take records home; however, in exceptional cases where this cannot be avoided, the records must be stored securely. Records should not be left in a car overnight but stored securely indoors.

Transmitting information by Email, Fax or Post

- ***Only use an official KCETB email address. Personal email addresses must NOT be used, eg: @hotmail, @yahoo, @gmail, etc***

- Always double-check that you are sending the email to the correct recipient.

- Ensure BCC Function on email is used if sending group messages. (It is advisable to enter your own email address in the "To" field and enter the email addresses of the group in the "Bcc" field in order to keep email addresses private).

- Always encrypt or password protect emails containing Personal Identifiable Data.

- Staff must respect the privacy of others at all times and only access fax messages where they are the intended recipient or they have a valid work-related reason.

- If a staff member receives a fax message and they are not the intended recipient, they must contact the sender and notify them of the error.

- Fax machines must be physically secured and positioned to minimise the risk of unauthorised individuals accessing the equipment or viewing incoming messages.

- Where possible, the information should be encrypted and transmitted via email.

It is acceptable to transmit confidential and personal information by fax only when:

1. All persons identified in the fax message have fully understood the risks and agreed.

2. There are no other means available.

Best practice is that the use of fax is discontinued or minimised as far as possible. However, the following steps are to be taken to maintain security and confidentiality when transmitting personal information by fax:

- The fax message must include a fax cover sheet.
- Only the minimum amount of information necessary should be included in the fax message.
- Before sending the fax message, contact the intended recipient to ensure he/she is available to receive the fax at an agreed time.
- Ensure that the correct number is dialled.
- Keep a copy of the transmission slip and confirm receipt of the fax message.
- Ensure that no copies of the fax message are left on the fax machine.

When using the postal system, if the mail item contains sensitive personal information:

- The envelope should be clearly marked "Strictly Private and Confidential".
- Information of this nature should be sent by registered post.
- Provide “return to sender” information in the event that the mail is undeliverable.
- Double-check that the contents in the envelope are for the intended person.
- Ensure that incoming and outgoing post is kept in such a manner to ensure confidentiality. Eg: Do not sort incoming post on office counters where unauthorised people could see it, or leave outgoing post, which shows the names and addresses of the recipients, visible while awaiting collection by An Post or awaiting delivery to the Post Office.

Password Protection is required on all devices

All passwords must be unique and must be a minimum of 8 characters. If existing systems are not capable of supporting 8 characters, then the maximum number of characters allowed must be used. Passwords must contain a combination of letters (both upper & lower case), numbers (0-9) and at least one special character (for example: “, £, $, %, ^, &, *, @, #, ?, !, €).
Passwords must not be left blank.

Users must ensure passwords assigned to them are kept confidential at all times and are not shared

with others including co-workers or third parties. In exceptional circumstances where a password has to be written down, the password must be stored in a secure locked place, which is not easily accessible to others.

Encryption of information

Confidential and personal information stored on shared KCETB network servers which are situated in physically unsecure locations, for example, remote file/print servers, must be protected by the use of strict access controls and encryption. All devices used for the storage and processing of personal data must be encrypted. It is the responsibility of each device owner to ensure that the device is appropriately secure.

KCETB specifically prohibits the storage of KCETB data on USB memory sticks.

- Where possible all confidential and personal information must be stored on a secure network server with restricted access. Where it has been deemed necessary by the information owner to store confidential or personal information on any device other than a KCETB network server, the information must be encrypted.

- Desktop computers, which for business or technical reasons need to store/host KCETB student or employee information systems and/or confidential or personal information locally (as opposed to a secure KCETB network server), must have KCETB-approved encryption software installed.

- Desktop computers used by employees to work from home (home working) must have KCETB-approved encryption software installed.

- All KCETB laptop computer devices must have KCETB-approved encryption software installed prior to their use within KCETB. In addition to encryption software, the laptop must be password protected and have up-to-date anti-virus software installed.

Mobile Phones

- Users must ensure their KCETB mobile phone device is protected at all times.

- At a minimum, all mobile phone devices must be protected by the use of a Personal Identification Number (PIN).

- Users must take all reasonable steps to prevent damage or loss to their mobile phone device. This includes not leaving it in view in an unattended vehicle and storing it securely when not in use. The user may be held responsible for any loss or damage to the mobile phone device, if it is found that reasonable precautions were not taken.

- Confidential and personal information must not be stored on a KCETB mobile phone device.

- Users must respect the privacy of others at all times, and not attempt to access KCETB mobile phone device calls, text messages, voice mail messages or any other information stored on a mobile phone device unless the assigned user of the device has granted them access.

- Mobile phone devices equipped with cameras must not be used inappropriately within KCETB offices, schools or centres or at any associated events.

- Confidential and/or personal information regarding KCETB, its employees or students must not be sent by text message.

- KCETB Staff should not have any work-related social media groups on their mobile phones/devices to avoid sharing of personal data.

- All email messages sent from a KCETB mobile phone device which contain confidential and/or personal information must be encrypted.

- Users must report all lost or stolen mobile phone devices to their line manager and to the Data Protection Office, 056 7770966.

Social Media

Please contact the ICT section before creating or altering any Social Media Platform.

Organisations providing services on KCETB's behalf

Where KCETB engages a third party to provide services on its behalf and where the services require the service provider to process personal data, KCETB is required by law to have a written contract in place with the service provider which provides sufficient guarantees with regard to data protection compliance.

KCETB is arranging detailed Services Agreements for these purposes, which will be available from KCETB Data Protection Office.

Disposal of records

It is vital that the process of record disposal safeguards and maintains the confidentiality of the records. This can be achieved internally or via an approved records shredding contractor, but it is the responsibility of the school/centre/office to satisfy itself that the methods used provide adequate safeguards against accidental loss or disclosure of the records.

KCETB staff may shred confidential records using in-house shredders. This shredded paper can be recycled as part of a recyclables collection.

If shredding off-site, confidential waste should be secure until collection by the shredding contractor. Confidential waste bags/wheelie bins should be exchanged by the shredding contractor, and shredded off-site at an agreed location. If confidential waste is transported off site, documents should never be legible by members of the public.

A Certificate of Destruction must be obtained from the shredding company after shredding and should be stapled/stored with the Register of Records as outlined below.

A register of records destroyed must be maintained as proof that the records no longer exist. The register should show:
- name of the file
- former location of file
- date of destruction
- who gave the authority to destroy the records.

Templates of these documents can be found in the KCETB Records Management Policy

Data Protection Breaches

If personal data is inadvertently released to a third party without consent, this may constitute a breach of the Data Protection Acts. If a staff member is aware of a breach or suspected breach of the Data Protection Act they must act in accordance with the KCETB Data Breach Protocol**.**

The first step is to notify the KCETB Data Protection Office, which will advise as to the steps to be followed.

Please note, the KCETB Data Protection Office will report Data Protection Breaches to the Data Protection Commissioner as required.

Further information in relation to the policies referred to in this document is available on www.kcetb.ie

Contact details for KCETB Data Protection Office:

Data Protection Office
Seville Lodge
Callan Road
Kilkenny
Tel: (056) 7770966

Remember

Personal data collected by staff in KCETB in the normal course of work must be:

- ✓ adequate, relevant and not excessive
- ✓ obtained and processed fairly
- ✓ kept only for one or more specified, explicit and lawful purposes
- ✓ used and disclosed only in ways compatible with these purposes
- ✓ kept safe and secure
- ✓ kept accurate, complete and up-to-date
- ✓ retained for no longer than is necessary for the purpose or purposes for which it was collected
- ✓ provided to the individual to whom it refers at their request.

Appendix – additional note

Filing Guidelines

1. Before filing a piece of paper, ask yourself, "Will I need this in the future?" Don't keep a piece of paper just on the chance that you may need it "someday."

2. Don't always save every draft of a document. For most purposes the final version is sufficient.

3. Don't file multiple copies of the same document, unless justified.

4. The originator normally keeps copies of reports and correspondence. Just because a document is sent to you doesn't oblige you to keep it indefinitely. If you need to see it again, ask the originator for another copy.

5. If, for example, records are scheduled for destruction after three years, don't store them for five years.

6. In general, records received from ETB schools/institutes/centres/offices should be filed under the name of the originating school/institute/centre/office.

7. Some records may belong under more than one series or category. To handle this, file the records in one category and place a cross-reference note in the other. It is important to be consistent in deciding where to file records. Once information is filed in a given series and category, it should always be filed there.

8. Label and date all files.

9. Colour-coding the different series is a useful tool, especially for refiling folders.

10. Create a file guide with a description of the filing system and instructions for the user so new personnel can continue to use the filing system easily. This will also avoid the arbitrary creation of new file folders.

11. Create cross-listings to help locate items. Create a file database on the PC using the file-folder heading, cross-listing, and location notes.

12. Spell out acronyms and abbreviations.

13. Sort records prior to filing.

14. Use staples rather than paper clips in folders.

15. Discard envelopes if the return address is available on the document itself. Most phone messages, illegible notes, and routine acknowledgements can also be discarded.

16. Do not overfill file folders. If they are overfilled, divide them into several folders with the same name and File number (e.g.: Maternity Leave Applications 2008/2009, File 1).

17. Do not overstuff file drawers. This can make retrieval of files difficult, as well as creating a dangerous work environment.

18. Check files regularly, using established retention schedules.

19. Consider using "Out Markers" when removing folders for use. This makes refiling much easier and lets others in the office know that a file exists so another is not created, who has the file, and when it was checked out.

CONFIRMATION FORM

I confirm that I have read the attached Data Protection Guidance and Data Protection Statement and that I understand what is required of me as a KCETB employee to ensure compliance with Data Protection Legislation

Name: _____

Title: _____

Location of centre: _____

Line Manager: _____

Date: _____

Signed: _____

This signed confirmation form to be kept on file by line manager.