cetb
Bord Oideachais agus Oiliúna Chorcaí
Cork Education and Training Board

Cork ETB
Data Breach Management Policy and Procedures

POLICY ON THE MANAGEMENT OF DATA BREACHES IN SCHOOLS/COLLEGES AND OTHER EDUCATION AND ADMINISTRATIVE CENTRES UNDER THE REMIT OF CORK EDUCATION AND TRAINING BOARD

Adopted by Cork Education and Training Board

At a meeting held on 22nd January 2015

1. Policy

1.1. Safeguarding personally identifiable information in the possession of Cork Education and Training Board (the "**ETB**") and preventing its breach is essential to ensure that the ETB retains the trust of staff, students and members of the public.

1.2. The ETB, as data controller, and appropriate data processors so contracted, are subject to the provisions of the Data Protection Acts, 1988 and 2003 and, as such, exercise due care and attention in collecting, processing and storing personal data and sensitive personal data provided by data subjects for defined use.

1.3. The ETB has prepared a **Data Protection Policy** and monitors the implementation of that policy at regular intervals. The ETB retains records (both electronic and manual) concerning personal data in line with its **Data Protection Policy** and seeks to prioritise the safety of personal data and particularly sensitive personal data, so that any risk of unauthorised disclosure, loss or alteration of personal data is avoided.

1.4. This document sets out the ETB's policy and procedures which shall be followed in the event of a breach of the security of the systems used by the ETB.

1.5. For the purpose of this policy, the term "**breach"** includes the loss of control, compromise, unauthorised disclosure or unauthorised access or potential access to personally identifiable information, whether in physical (paper) or electronic form. A data security breach can happen for a number of reasons, including:-

- loss or theft of data or equipment on which data is stored (including break-ins to any of our premises);
- inappropriate access controls allowing unauthorised use;
- equipment failure;
- human error;
- unforeseen circumstances such as flood or fire;
- a hacking attack;
- Access where information is obtained by deceiving the organisation that holds it.

1.6. The ETB, as a "**Data Controller**", will make all reasonable efforts to protect confidential information and specifically personal data, when it acts in that capacity.

1.7. The ETB will make all reasonable efforts to protect such information under the ETB's control from unauthorised access, use, disclosure, deletion, destruction, damage or removal. Although reasonable efforts are made to protect facilities, equipment, resources and data, the possibility that the security of data, maintained by the ETB, may be breached exists. As a result, this Policy sets out a breach notification procedure or action plan to be implemented should the security procedures in place not prevent a data breach**.**

2. Purpose

2.1. The purpose of this Policy is to acknowledge the importance of information security, to recognise that a breach may still occur and, therefore, to establish a framework for addressing any such breach.

2.2. This Policy applies to *Cork ETB* as *data controller.* The Policy will be

2.2.1. available on the ETB website, *www.cork.etb.ie*

2.2.2. circulated to all appropriate data processors and incorporated as part of the service-level agreement/data processing agreement between the ETB and the contracted company, and

2.2.3. Advised to staff at induction and at periodic staff meetings or training sessions organised by the ETB.

3. Scope

3.1. This policy applies to all personnel in schools/colleges and other education and administrative centres under the remit of the ETB.

4. Responsibility

4.1. Cork ETB staff is responsible for ensuring that appropriate and adequate protection and controls are in place and applied in each facility and resource under their control and for identifying areas where they are not. The Chief Executive, PO, APO, Principals, Centre Managers and Heads of Department are responsible for ensuring that staff follow this Policy and adhere to all related procedures.

4.2. Periodic reviews of the measures and practices in place shall be carried out.

5. Notification of a Breach – Each Staff Member's Duty to Notify

5.1. As soon as a member of ETB staff becomes aware that personal data has been compromised (e.g. through loss of a portable device, misaddressing of correspondence, sensitive information left where unauthorised viewing could take place – e.g. photocopies not properly disposed of or left on a copier), the ETB member of staff shall:

5.1.1. Immediately notify the Principal/Manager/Director or CE, and

5.1.2. Complete the **Data Security Breach Incident Report** (See Appendix 1).

5.2. The ETB Principal/Manager/Director who receives the notification shall investigate the circumstances surrounding the breach. The seriousness of the breach will determine the type of investigation that will take place. It may include an on-site examination of systems and procedures. In the event of a serious data security breach, the ETB Principal/Manager/Department Head will escalate the matter, the Breach Management Team will be informed and contact will be made with the Office of the Data Protection Commissioner for advice and clarification.

5.3. Where appropriate, the Breach Management Team will put a communication plan in place to contact the owner of the data involved (the *data subject*). Security of the medium used for notifying individuals of a breach of data protection procedures and the urgency of situation should be borne in mind. Specific and clear advice should be given to individuals on the steps they can take to protect themselves and also on what the ETB can do to assist them.

6. Protocol for Action in the Event of Breach

In circumstances where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the ETB will apply the following protocol**:**

6.1. The ETB will seek to contain the matter and mitigate any further exposure of the personal data held. The ETB shall have regard to the "Incident Response DOs and DON'Ts for IT systems" advice set out at **Appendix 2**. Depending on the nature of the threat to the personal data, this may involve a quarantine of some or all PCs, networks etc. and a request that staff do not access PCs, networks etc. Similarly, it may involve a quarantine of manual records storage areas and other areas as may be appropriate. By way of a preliminary step, an audit of the records held or backup servers should be undertaken to ascertain the nature of what personal data may potentially have been exposed.

6.2. Where data has been "damaged" (as defined in the Criminal Justice Act 1991, e.g. as a result of hacking), the matter must be reported to An Garda Síochána. Failure to do so will constitute a criminal offence in itself ("withholding information") pursuant to section 19 Criminal Justice Act, 2011. The penalties for withholding information include a fine of up to €5,000 or 12 months' imprisonment on summary conviction.

6.3. Where the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the ETB may conclude that there is no risk to the data and, therefore, no need to inform data subjects or to contact the Office of the Data Protection Commissioner. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

6.4. Depending on the nature of the personal data at risk and, particularly, where sensitive personal data may be at risk, the assistance of An Garda Síochána should be immediately sought. This is separate from the statutory obligation to report criminal damage to data arising under section 19 Criminal Justice Act 2011 as discussed at (6.2) above.

6.5. Contact should be made immediately with the ETB IT Department and with the data processor responsible for IT support in the ETB.

6.6. In addition and where appropriate, contact may be made with other relevant bodies such as the HSE, financial institutions, etc.

6.7. **Reporting of incidents to the Office of Data Protection Commissioner**: All incidents in which personal data (and sensitive personal data) have been put at risk shall be reported to the Office of the Data Protection Commissioner as soon as the ETB becomes aware of the incident (or within two working days), save in the following circumstances:

- When the full extent and consequences of the incident have been reported, without delay, directly to the affected data subject(s); **and**
- The suspected breach affects no more than 100 data subjects; **and**

- It does not include sensitive personal data or personal data of a financial nature[1].

Where all three criteria are not satisfied, the ETB shall report the incident to the Office of the Data Protection Commissioner within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident (see contact details below).

Data Protection Commissioner
Office of the Data Protection Commissioner
Canal House, Station Road, Portarlington, Co. Laois
Tel: 1890 252 231
Email: info@dataprotection.ie
Website: www.**data**protection.ie

Where no notification is made to the Office of the Data Protection Commissioner, the ETB shall keep a **summary record of the incident** which has given rise to the risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record shall comprise a brief description of the nature of the incident and an explanation as to why the CE did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records shall be provided to the Office of the Data Protection Commissioner upon request.

6.8. The ETB shall gather a small team of persons together to assess the potential exposure/loss. This team will assist the CE, the ETB's Data Protection Officer, (and the Principal/Manager/Director of the ETB school/Centre/Programme where relevant) with the practical matters associated with this Policy and Procedures. Action shall be taken in accordance with the CE's direction and advice. Each team member shall have a backup member of staff to cover holidays, sick leave etc.

NAME	LOCATION	CONTACT NUMBER
Ted Owens, Chief Executive	ETB Head Office, 21 Lavitt's Quay, Cork	021 4907000
Martin Hallahan, PO	ETB Head Office, 21 Lavitt's Quay, Cork	021 4907000
Suzanne Mullins, Head of HR	ETB Head Office, 21 Lavitt's Quay, Cork	021 4907000
Mary O'Leary, Head of Finance	ETB Head Office, 21 Lavitt's Quay, Cork	021 4907000
Adrian Deasy, Head of IT	ETB Head Office, 21 Lavitt's Quay, Cork	021 4907000
Una Carroll/Niall Kennefick, Head of Corporate Services	ETB Head Office, 21 Lavitt's Quay, Cork	021 4907000

[1] 'personal data of a financial nature' means an individual's last name, or any other information from which an individual's last name can reasonably be identified, in combination with that individual's account number, credit or debit card number.

Liz Donnelly, Data Protection Officer	ETB Head Office, 21 Lavitt's Quay, Cork	021 4907000
Brendan Drinan, Principal	Schull Community College	028 28315
Padraig O'Sullivan, Deputy Principal	Schull Community College	28 315

6.9. The team will, under the direction of the CE, give immediate consideration to informing those affected[2]. At the direction of the CE, the team shall contact the individuals concerned (whether by phone/email etc.) to advise that an unauthorised disclosure/loss/destruction or alteration of the individual's personal data has occurred.

6.10. Where possible and as soon as is feasible, the data subjects (i.e. individuals to whom the data relates) should be advised of:

6.10.1. the nature of the data that has been potentially exposed/compromised;

6.10.2. the level of sensitivity of this data;

6.10.3. the steps which the ETB intends to take by way of containment or remediation; and

6.10.4. Whether the ETB intends to contact other organisations and/or the Office of the Data Protection Commissioner.

6.10.5. Where individuals express a particular concern with respect to the threat to their personal data, this should be back to the CE who may, advise the relevant authority e.g. Gardaí, TUSLA etc.

6.10.6. Where the data breach has caused the data to be "damaged" (e.g. as a result of hacking), the CE shall contact An Garda Síochána and make a report pursuant to Section 19 Criminal Justice Act 2011.

6.10.7. The CE shall notify the ETB's insurers that there has been a personal data security breach.

6.11. **Contracted Companies Operating as Data Processors**: Where an organisation, contracted and operating as a *data processor* on behalf of the ETB, becomes aware of a risk to personal/sensitive personal data, the organisation will report this directly to the ETB as a matter of urgent priority. In such circumstances, the CE should be contacted directly (and in the case of an ETB School/Centre/Programme, the relevant Principal/Manager/Director should also be contacted). This requirement should be

[2] Except where law enforcement agencies have requested a delay for investigative purposes. Even in such circumstances consideration should be given to informing affected data subjects as soon as the progress of the investigation allows. Where Cork ETB receives such a direction from law enforcement agencies, they should make careful notes of the advice they receive (including the date and the time of the conversation and the name and rank of the person to whom they spoke). Where possible, Cork ETB should ask for the directions to be given to them in writing on letter-headed notepaper from the law enforcement agency (e.g. An Garda Siochána), or where this is not possible, Cork ETB should write to the relevant law enforcement agency to the effect that "we note your instructions given to us by your officer [insert officer's name] on XX day of XX at XX pm that we were to delay for a period of XXX/until further notified by you that we are permitted to inform those affected by the data breach."

clearly set out in the appropriate data protection section in the data processing agreement/contract.

6.12. A full review should be undertaken and, having regard to information deriving from the experience of the data breach, staff should be advised of any changes to this policy and of upgraded security measures. Staff should also receive refresher training where necessary.

6.13. **What may happen arising from a report to the Office of Data Protection Commissioner?**

6.13.1. Where any doubt may arise as to the adequacy of technological risk-mitigation measures (including encryption), the ETB shall report the incident to the Office of the Data Protection Commissioner within **two working days** of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact will be by e-mail, telephone or fax and shall **not** involve the communication of personal data.

6.13.2. The Office of the Data Protection Commissioner will advise the ETB of whether there is a need for the ETB to compile a detailed report and/or for the Office of the Data Protection Commissioner to carry out a subsequent investigation, based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

6.13.3. Should the Office of the Data Protection Commissioner request the ETB to provide a detailed written report into the incident, the Office of the Data Protection Commissioner will specify a timeframe for the delivery of the report into the incident and the information required. Such a report should reflect careful consideration of the following elements:

- the amount and nature of the personal data that has been compromised;
- the action being taken to secure and/or recover the personal data that has been compromised;
- the action being taken to inform those affected by the incident or reasons for the decision not to do so;
- the action being taken to limit damage or distress to those affected by the incident;
- a chronology of the events leading up to the loss of control of the personal data; and
- The measures being taken to prevent repetition of the incident.

6.13.4. Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where the ETB has not already done

so. If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.

7. Media Enquiries

7.1. Media enquiries about the breach shall be dealt with by authorised personnel only. A centralised "Fact Sheet" should also be created to ensure that one version, not many, becomes the view of the organisation internally and in contacts with the media.

8. Links with other documents and ETB Policies

8.1. Data Protection Act 1988 and (Amendment) Act 2003.
8.2. Data Protection Commissioner's Personal Data Security Breach Code of Practice.
8.3. Cork ETB Data Protection Policy.
8.4. Cork ETB ICT Acceptable Usage Policy.
8.5. Cork ETB CCTV Policy.
8.6. Cork ETB Employee Handbook

9. Implementation & Review

This policy was adopted by Cork ETB on 22/1/2015 which is the date of implementation. The policy will be reviewed annually and in light of changes in legislation, legal advice and as relevant new technologies emerge.

cetb
Bord Oideachais agus Oiliúna Choreai
Cork Education and Training Board

Appendix 1
Data Security Breach – Incident Report

Breach ID:

When did the breach take place?

When was the breach discovered?

Who reported the breach?

Were there any witnesses? If Yes, state Names.

Please provide details of the breach:

Were any IT systems involved? If so please list them.

I

Any additional comments?

Signed:_____

Date: _____ **Time:** _____

For Breach Management Team Use

Details logged by _____

Severity of the breach (0 being minor, 5 being critical)

0 1 2 3 4 5

Data Subjects to be notified Yes ☐ No ☐

Details:_____
_____

Data Protection Commissioner to be notified Yes ☐ No ☐

Details (Date/time, note of advice received):_____
_____

Gardaí to be notified Yes ☐ No ☐

Details: _____

Appendix 2

Incident Response DOs and DON'Ts for IT systems

DOs

- Immediately isolate the affected system to prevent further intrusion, release of data, damage etc.
- Use the telephone to communicate. Attacker may be capable of monitoring e-mail traffic.
- Preserve all pertinent logs, e.g. firewall, router and intrusion detection system.
- Make backup copies of damaged or altered files and keep these backups in a secure location.
- Identify where the affected system resides within the network topology.
- Identify all systems and agencies that connect to the affected system.
- Identify the programs and processes that operate on the affected system(s), the impact of the disruption and the maximum allowable outage time.
- In the event that the affected system is collected as evidence, make arrangements to provide for the continuity of services i.e. prepares redundant system and obtain data backups.

DON'Ts

- Delete, move or alter files on the affected systems.
- Contact the suspected perpetrator.
- Conduct a forensic analysis.

This Data Breach management Policy was reviewed by the Board of Management.

This Policy was agreed on _____07/06/2016_____.

Signed _____Noel Coakley_____ Signed _____Brendan Drinan_____

Chairperson of BOM Principal

Date ___07/06/2016_____

Date of next review _____07/06/2021