etb
Bord Oideachais agus Oiliúna
an Chabháin agus Mhuineacháin
Cavan and Monaghan
Education and Training Board

CAVAN AND MONAGHAN EDUCATION AND TRAINING BOARD

Data Breach Management Policy

Adopted by Cavan and Monaghan Education Training Board

on 11 September 2013

Policy

Safeguarding personally identifiable information in the possession of **Cavan and Monaghan Education and Training Board** (the ETB) and preventing its breach is essential to ensure The ETB retains the trust of both staff and the public. The ETB has in place a Data Breach Notification Policy/Plan including procedures that address both the protection of certain information, including "Personal Information" as defined in the Data Protection Act 1988 and Amendment Act 2003, and the prompt notification of those individuals actually or potentially affected by a breach of the security of the systems used by the ETB.

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.

The ETB will make all reasonable efforts to protect confidential information and specifically non-public personal information as a "Data Controller" when it acts in that capacity.

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, there exists the possibility that the security of data maintained by the ETB may be breached. As a result, this policy requires that the ETB has a reasonable and appropriate breach notification procedure or action plan in place should security procedures not prevent a breach**.**

This policy should be read in conjunction with the Data Protection Commissioner's Personal Data Security Breach Code of Practice and the Code of Practice for the Protection of Personal Data in ETBs.

Purpose

The purpose of this policy is to acknowledge the importance of information security and to recognise that a breach may still occur and therefore to establish a framework for addressing a breach that occurs.

Scope

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

1.0 Responsibility

ETB staff are responsible for ensuring that appropriate and adequate protection and controls are in place and applied in each facility and resource under their control and identifying those that are not. Chief Executive, APO, Principals, Centre Managers and Heads of Department are responsible for ensuring that staff follow the intent of this Policy and are adhering to all related procedures.

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

2.0 Data Security[1]

High standards of physical and technical security are essential to protect the confidentiality of personal data. These include:

- ensuring access to information is restricted to authorised staff in accordance with defined policy
- ensuring computer systems are password protected
- keeping information on computer screens and paper files hidden from callers to offices[2]
- ensuring that no documentation of a "confidential/sensitive nature" is left on desks/photocopiers etc.
- ensuring that personal data is protected by strong encryption when being stored on portable devices or transferred electronically (including email)
- ensuring that personal data is not stored on portable devices except in essential circumstances. Where deemed essential, the data must be encrypted and a record kept of the nature and extent of the data and why it is being stored on a portable device. Arrangements should be put in place to fully delete the data on the portable device when it is no longer being used
- having appropriate facilities in place for disposal of confidential waste
- non-disclosure of personal security passwords to any other individual (including other employees within the organisation)
- keeping premises secure, especially when unoccupied
- keeping audit logs in relation to read access, changes, additions deletions on ICT system
- having adequate security measures and policies in place in relation to the use of laptops and other mobile storage devices
- inserting appropriate data protection and confidentiality clauses in arrangements with any processors of personal data on the organisation's behalf, including:
  - the conditions under which data may be processed
  - the minimum security measures that the data processors must have in place
  - mechanisms or provisions that will enable the data controller to ensure that any data processor is compliant with the security practices which include a right of inspector or independent audit

3.0 Breach Incident Handling and Reporting Requirements

When faced with a breach of security incident the ETB must be able to respond in an appropriate manner protecting both its own information and helping to protect the information of others who might be affected by the incident. The ETB's Data Breach Notification Policy/Plan outlines the roles and responsibilities of relevant personnel, in the prevention of security breaches and in dealing with threats of breaches or actual breaches and responding by implementing the appropriate recovery and reporting procedures.

4.0 Data Breach Notification Policy/Plan

It is necessary for the ETB, in the course of its business, to collect and use data (information in a form which can be processed) for a variety of purposes, about its staff, students and other individuals with whom they come in contact.

[1] This section should be read in conjunction with the ICT Acceptable Use Policy.

Due to the increasing frequency of information security breaches it is important that staff understand the repercussions a data security breach can have on the ETB – from the moment the breach is detected to the way we respond after the breach occurs.

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-in 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.

The ETB has adopted the following plan for use in the event of data breaches:

(i) Identification and Classification

Staff must be made fully aware as to what constitutes a breach, how it may occur, who to contact when one happens and how to log the details.

A Breach Management Team (BMT) must be established with representatives from each School/Centre/Office within the ETB, as well as a team leader with decision making authority. The team will evaluate all breaches, their impact and formulate a plan on how to proceed. Each team member will have a backup member to cover holidays, sick leave etc.

(ii) Containment & Recovery

Containment involves limiting the scope and impact of the breach of data protection procedures.

The Breach Management Team will evaluate the breach; determine what damage may be caused, and then try to limit the damage and impact caused by the breach. The team will make recommendations to ensure such an incident cannot happen again.

The Breach Management Team leader will be responsible for ensuring that the required resources are in place to investigate the breach and will take the lead in the investigation. If specialist resources (IT, Legal, Financial etc) are required the BMT leader will get them involved as soon as possible.

Relevant the ETB staff will be notified of the breach and how they are to help in the investigation.

The Breach Management Team will decide whether to notify data subjects and if so this should be done without delay.

Should a serious breach take place the team leader will contact the Gardaí and Data Protection Commissioner and act as liaison with them.

(iii) Incident Response DOs and DON'Ts for IT systems

DO'S

- 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 back-up 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 the affected system is collected as evidence, make arrangements to provide for the continuity of services i.e. prepare redundant system and obtain data back-ups.

DON'Ts

- delete, move or alter files on the affected systems
- contact the suspected perpetrator
- conduct a forensic analysis

(iv) Risk Assessment

Assessing the risk will depend on how likely it is that adverse consequences will materialise, and in the event of materialising, how serious or substantial they are likely to be. The following needs to be considered:

1. the type of data involved e.g. personal, financial or medical
2. how long the breach has been going on. How sensitive the data is? Some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
3. if data has been lost or stolen, was encryption or other protection methods in place?
4. what has happened to the data? If data has been stolen it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been altered or damaged, this poses a different type and level of risk
5. how many individuals are affected?
6. what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic thief while the loss of apparently trivial piece of information could help a fraudster build up a detailed picture for identity theft
7. who are the individuals whose data has been breached?

8. what harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these as well as other aspects of their life?
9. are there wider consequences to consider such as loss of public confidence in the service we provide?
10. if information has been deleted can it be retrieved from backup systems?

(v) Notification of a Breach

As soon as personal data for which you are responsible has been compromised – e.g. through loss of a portable device, misaddressing of labels, sensitive information left where unauthorised viewing could take place – i.e. photocopies not properly disposed off or left on copier, you should complete the Data Security Breach Incident Report and immediately notify your Principal/Manager/Director who will investigate the issues 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 Breach Management Team will be informed and contact will be made with the Office of the Data Protection Commissioner for advice and clarification.

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 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 what the ETB is willing to do to assist them. Provision of a helpline number or a web page should be considered. Notifications may be delayed if the Gardaí advise that it will impede an investigation.

(vi) Media

Media enquiries about the breach should 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.

The ETB should consider notifying third parties such as the Gardaí, bank or credit card companies who can assist in reducing the risk of financial loss to individuals.

(vii) Evaluation and Response

Subsequent to any information security breach a thorough review of the incident should occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

Any recommended changes to policies and/or procedures should be documented and implemented as soon as possible thereafter.

The plan will also be reviewed periodically as new issues and technologies may arise which will have a bearing on the way it is implemented.

(viii) Implementation & Review

This policy was adopted by Cavan and Monaghan ETB on 11 September 2013 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.

5.0 Breach Management Team

NAME	LOCATION	CONTACT NUMBER
Martin G. O'Brien	Chief Executive	047 30888
Patricia Monahan	APO Monaghan Office	047 30888
Maura Smith	APO Cavan Office	049 4331044
Head of Finance		
Head of HR		
Head of Corporate Services		
Fiona Nugent	Data Protection Officer	047 30888
Principal/Director/Co-ordinator	School/Institute/Centre/Office	As appropriate
Other relevant staff	As appropriate	As appropriate

6.0 Contact Details

Cavan and Monaghan ETB
Administration Centre
Market Street
Monaghan
Co Monaghan
Tel: 047 30888
Email: xxxx
Website: xxxx

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

7.0 References

- Data Protection Act 1988 and (Amendment) Act 2003
- Data Protection Commissioner's Personal Data Security Breach Code of Practice
- Cavan and Monaghan ETB Data Protection Policy
- Cavan and Monaghan ETB ICT Acceptable Usage Policy
- Cavan and Monaghan ETB CCTV Policy
- Code of Practice for the Protection of Personal Data in ETBs.

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.

Is any additional material available e.g. error messages, screen shots, log files, CCTV?

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:_____
_____