Data Security Breach – Incident Report

CONFIDENTIAL

The GDPR defines a "personal data breach" in Article 4(12) as: "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".

Breach ID:

When did the breach take place?

Where did the breach take place?

e.g. Location of breach

When was the breach discovered?

e.g. Specific time & date

Who reported the breach?

Contact details of person who reported the breach?

Was the Data Protection Officer immediately contacted?

Yes ☐ **No** ☐

If YES, state by what means (e.g. phone, email etc.) and the time and date of the contact made?

If NO, was any other senior official e.g. CE, Director etc. contacted and if so, by what means (e.g. phone, email etc.) and the time and date of the contact made?

Were there any witnesses? If Yes, state Names & phone contact details

Please provide details of the breach:

What was the nature of the breach?
What categories of data subjects (e.g. students, adult learners, parents/guardians; other vulnerable groups, employees, board members; contractors etc.) were affected and/or potentially affected by the breach?
Approximate number of data subjects affected:
Categories of personal data/records (e.g. health data, education records, social care information, financial details, bank account numbers, passport numbers etc):
Approximate number of personal data records concerned:
Description of the likely consequences of the personal data breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy etc.):
Description of the measures undertaken (or proposed to be undertaken) by the ETB to address the breach (including, where appropriate, measures to mitigate its possible adverse effects):

Important note: where the exact details of any of the above are not yet known, this shall not delay a timely breach notification to the DPC. Further information can follow, when available: "*the information may be provided in phases without undue further delay*[1]".

Was the breached data protected through passwords, encryption etc.? Supply details below.

In your opinion, is the breach likely to be of a temporary nature? Can the personal information exposed be recovered?

Were any IT systems involved? (e.g. email, website, school admin system, VS Ware, Facility, apps). If so, please list them.

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

Have you taken any action/steps so far to seek to stop/mitigate the risk either to the data subject/s who you think have been affected OR any other additional data subjects you consider may be affected? If YES, please describe below

[1] Article 33(4) GDPR.

Have you spoken to someone in ETB management team at administrative head office level e.g. CE, Director, Head of IT etc?
If so, please advise whom you contacted, and a brief outline of the advice given by him/her.

Have you made any contact with any external agencies e.g. Insurance Company, IT provider, Gardaí etc.? If YES, please describe below specifically whom you contacted and supply the name and contact details of same.

Any additional comments?

Signed:	
Your position in the ETB:	
Name of school, office, centre:	
Your contact number (ideally mobile number):	
Date:	
Time of completion:	

Thank you for your efforts in completing this form. The effort undertaken in its completion will help the ETB in its further investigation/analysis of the matter.

Please ensure this is forwarded directly to the ETB Data Protection Officer
Email: dataprotection@kwetb.ie Phone: 045 988 000
Post to: KWETB, Áras Chill Dara, Devoy Park, Naas, Co. Kildare

CONFIDENTIAL - THIS FORM HAS BEEN COMPLETED IN CONTEMPLATION OF LEGAL PROCEEDINGS

For your reference

Breaches can be categorised according to the following three well-known information security principles:

(a) "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
(b) "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
(c) "Availability breach" - where there is an accidental or unauthorised loss of access15 to, or destruction of, personal data.

Depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these. Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

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
- contact the ETB Data Protection Officer without delay <Insert contact details>
- 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.

For Breach Management Team Use Only **Details logged by:**	*Insert details in column below*
DPO Name:	
Time & date of receipt by ETB of this form	
Type of personal data breach *e.g. Confidentiality breach; integrity breach; availability breach (see examples)*	
Numbers of likely people affected by the breach	*Estimated number of data subjects affected?* *Types of data affected?*
Were special categories (e.g. sensitive personal data) compromised in the breach? *Special categories i.e.* *Racial or ethnic origin* *Political opinions* *Religious or philosophical beliefs* *Membership of a trade union* *biometric and genetic data,* *health* *sex life or sexual orientation.*	**Yes** ☐ **No** ☐ *Insert any relevant information below e.g. How many data subject(s) sensitive personal data has been affected?* *What type of sensitive personal data was breached?*
Severity of the breach *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.* **Rate the breach opposite in terms of its likely severity on the rights and freedoms of affected or potentially affected data subject/s i.e.** **High Risk** **Medium Risk** **Low / No Risk*** * **If it is assessed that there is "no risk", the reasons for that decision must be recorded.**	  

CE and or members of the senior management team to be notified	**Yes** ☐ **No** ☐
IT Service Providers / IT support to be notified	**Yes** ☐ **No** ☐
Insurance Company to be notified	**Yes** ☐ **No** ☐
Gardaí to be notified	**Yes** ☐ **No** ☐
Legal advisors to be notified (including LSSU as determined by ETB)	**Yes** ☐ **No** ☐
Data Subjects to be notified? *How many?* *Is there a list of contact details for data subjects?* *If not, can we recover?*	**Yes** ☐ **No** ☐
Supervisory Authority to be notified? *Contact details for Supervisory Authority* Data Protection Commission Telephone: +353 57 8684800 +353 (0)761 104 800 Lo Call Number: 1890 252 231 Fax: +353 57 868 4757 E-mail: info@dataprotection.ie Postal: Data Protection Commission Canal House Station Road Portarlington R32 AP23 Co. Laois	**Yes** ☐ **No** ☐ *If YES, list date and time of notification and any advice/instruction given by the Supervisory Authority:*
Any additional relevant additional details	
Signed by DPO:	
Signed by CE / nominee:	
Date:	

CONFIDENTIAL - THIS FORM HAS BEEN COMPLETED IN CONTEMPLATION OF LEGAL PROCEEDINGS