



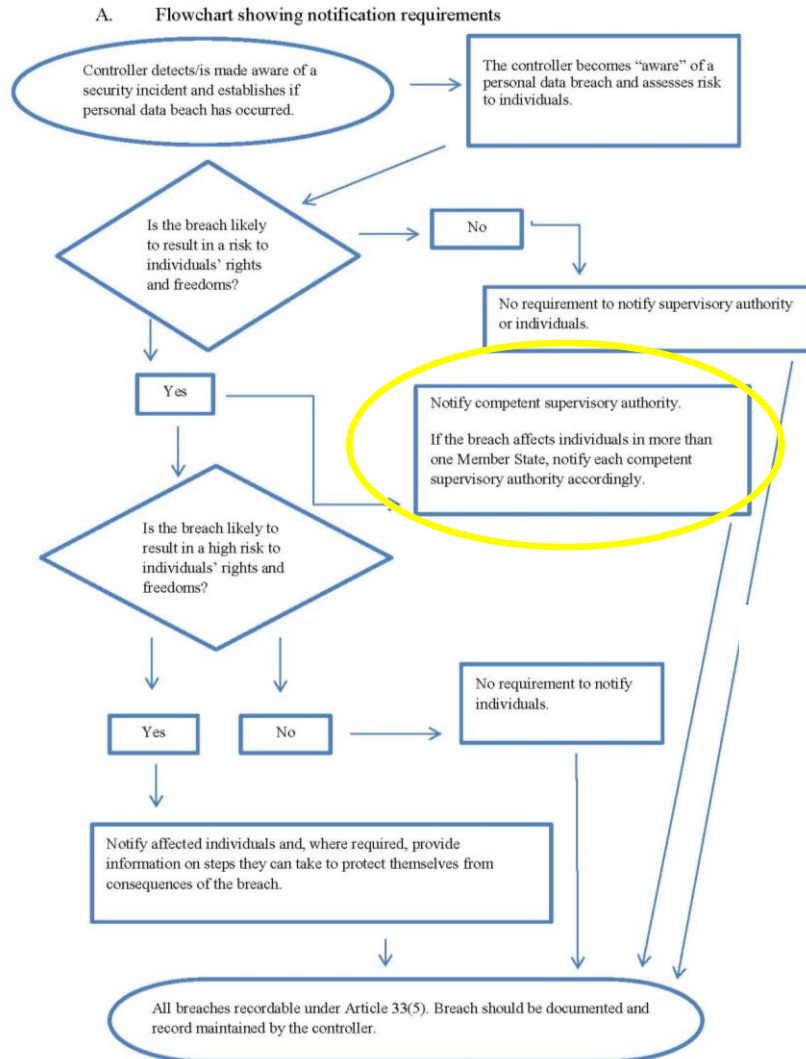
Bord Oideachais agus Oiliúna Dublin and Dún Laoghaire
Átha Cliath agus Dhún Laoghaire Education and Training Board

Data Breach Protocol

Version number	1
Policy drafted by	Corporate Services
Approved by Executive on	11 th January 2021
Date on which it became operational	11 th January 2021
Next review date	11 th January 2022

1. Data breach and purpose of protocol

- 1.1. DDLETB has developed this personal data breach protocol. This is part of our strategic planning to ensure that DDLETB is prepared to respond in a personal data breach situation. The focus of any breach response plan will be on prompt action in order to protect individuals and their personal data. DDLETB is committed to:
 - (a) Notifying the Data Protection Commission (DPC) of a personal data breach without undue delay and not later than **72 hours** after becoming aware of it (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons).
 - (b) Notifying affected data subjects without undue delay, unless the personal data breach is unlikely to result in a high risk to the rights and freedoms of natural persons.
- 1.2. This protocol will be:
 - (a) circulated to all appropriate data processors. Data processors are required to alert the ETB immediately if the processor becomes aware of a breach of the personal data it is processing on behalf of the ETB
 - (b) advised to staff at induction and at periodic staff meetings/ training.
- 1.3. The following flow-chart (taken from the Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, Adopted on 3 October 2017) summarises the steps to be taken:



26

1.4. Definitions:

In this protocol, the following terms shall have the following meanings¹:

- 1.4.1. **“Aware”**: a data controller should be regarded as having become “aware” when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.
- 1.4.2. **“Damage”**: the personal data has been altered, corrupted, or is no longer complete.
- 1.4.3. **“Destruction”**: the data no longer exist or no longer exist in a form that is of any use to the controller.
- 1.4.4. **“Loss”**: the data may still exist but the controller has lost control or access to the data, or no longer has the data in its possession.
- 1.4.5. **“personal data breach”**: per Article 4(12) GDPR: “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”.
- 1.4.6. **“Temporary loss of data”**: an incident resulting in personal data being made unavailable for a period of time.
- 1.4.7. **“unauthorised or unlawful processing”** may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

¹ Definitions taken from GDPR and WP250 (“Guidelines on Personal data breach notification under Regulation 2016/679).

- 1.5. A data security breach can happen for a number of reasons, including:
- Human error.
 - Loss or theft of paperwork, or any device containing data.
 - Break-ins, burglary, mugging.
 - Inappropriate access controls allowing unauthorised use/access.
 - Equipment failure and inadequate system back-ups.
 - A disaster such as flood or fire.
 - Phishing or blagging (where information is obtained by deception or spoofing).
 - Malicious attacks such as hacking or ransomware attack.
- 1.6. Personal data breaches can result in adverse effects on individuals which can result in physical, material, or non-material damage. This could include causing the data subject embarrassment, distress, or humiliation. Other adverse effect could include: *“loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, significant economic or social disadvantage²”* to affected individuals.
- 1.7. Personal data breaches can also be damaging to the ETB as they can result in:
- Damage to the relationship of trust we have built with staff and students,
 - Loss of, deletion of, or damage to personal data which is essential to the administration of the ETB,
 - Damage to the reputation of DDLETB
 - Administrative fines in accordance with the provisions of Data Protection legislation, enforcement action, and/or litigation.

2. Protocol

In case of a personal data breach, the DDLETB will follow the following protocol:

2.1. Identify that there is an issue an alert the relevant people

2.1.1. The DPO³ shall be notified as soon as possible.

2.1.2. The DPO shall notify the Chief Executive as soon as possible.

Emergency contact numbers:

If you have any queries, please consult our Data Protection Policy (available at www.ddletb.ie) or contact us at dataprotection@ddletb.ie.

2.1.3. The DPO shall gather together a small team to assess the potential exposure/loss and undertake appropriate containment/mitigation/remediation measures. All staff and all data processors and/or joint data controllers are required to give all necessary assistance to the DPO and this team.

2.1.4. The DPO shall start a written chronology of events, recording all relevant matters,

² Page 8, WP250.

³³ DPO appointed on an interim basis

including:

- (a) Date and time of notification of the breach (using the format DD/MM/YYYY and am/pm as appropriate).
 - (b) If the notification relates to a potential breach, details of any preliminary investigation (if required) in order to establish whether or not a breach has in fact occurred.
 - (c) Details of who reported the matter.
 - (d) Details of what was known/suspected at that initial stage.
 - (e) Details of what system/data-set is involved.
 - (f) Assessment of risk to the rights and freedoms of natural persons.
 - (g) Immediate actions undertaken (investigation, containment, mitigation, recovery, etc).
 - (h) Details of the team gathered to assist.
 - (i) Details of the tasks allocated to each team member.
 - (j) At the same time as (g), notification to DPC within 72 hours after having become aware.
 - (k) Notification to the affected individuals (if required) without undue delay
- 2.1.5. Regardless of whether (or not) a decision is made to notify the DPC, all documentation relating to documenting a (potential/reported/suspected) personal data breach including but not limited to the documentation required by Article 33(5) GDPR shall be stored on the ETB Risks Register.

2.2. **Containment, mitigation, and recovery**

- 2.2.1. DDLETB will immediately seek to contain the matter (insofar as that is possible) and shall take all necessary steps to mitigate any further exposure of the personal data held.
- 2.2.2. Where the data breach relates to an IT system and/or electronic data, contact shall be immediately made with the data processor responsible for IT support in DDLETB. Their advices and assistance should be sought in relation to appropriate measures of containment, quarantine, preservation of data and logs etc.
- 2.2.3. Depending on the nature of the breach/threat to the personal data, this may involve:
- (a) a quarantine of some or all PCs, networks etc.
 - (b) directing staff not to access PCs, networks, devices etc.
 - (c) suspending accounts,
 - (d) audit of the records held on backup server/s,
 - (e) ascertain the nature of what personal data may potentially have been exposed.
- 2.2.4. Consider a quarantine of manual records storage area/s and other areas as may be appropriate.
- 2.2.5. In appropriate cases, immediate consideration should be given to retaining an IT forensics specialist and obtaining legal advice.

2.3. **Assess Risk**

- 2.3.1. The ETB shall undertake an assessment in relation to the risk: is the personal data breach likely to result in a risk to the rights and freedoms of natural persons?
- 2.3.2. Classification of that risk:
- No risk?
 - Risk?
 - High risk?
- If it is assessed that there is “no risk”, the reasons for that decision must be recorded.
- 2.3.3. When assessing risk, the ETB shall have due regard to the sensitivity of the data and the category of the data subject (e.g. child, vulnerable person) in order to ascertain whether they may be placed at greater risk because of the breach.
- 2.3.4. The ETB may not be required to notify the DPC and data subjects if the breach is unlikely to result in a risk to their rights and freedoms, e.g. the data were securely encrypted with state-of-the-art encryption, and the key was not compromised in any security breach.

2.3.5. The ETB shall have regard to the recommendations made by the European Union Agency for Network and Information Services (ENISA) for a methodology in assessing the severity of a breach⁴.

2.3.6. If a decision is taken not to notify the DPC and/or affected data subjects, the justifications for that decision will be documented and stored on the ETB Risks Register.

2.4. Notification

2.4.1. **Reporting of incidents to the Data Protection Commissioner (“DPC”)**: All incidents in which personal data and sensitive personal data has been put at risk shall be reported to the Data Protection Commission without undue delay and where feasible, not later than **72 hours** after having become aware of it unless it does not result in a risks to the rights and freedoms of data subjects.

DPC Contact details

Telephone: 0761 104 800
Lo Call Number: 1890 252 231
E-mail: info@dataprotection.ie
Address: Data Protection Commission
Canal House, Station Road, Portarlinton
R32 AP23
Co. Laois

2.4.2. At a minimum, the initial notification to the DPC shall contain the following:

- The nature of the personal data breach.
- The categories of data subjects (e.g. children, other vulnerable groups, people with disabilities, employees, customers).
- 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.
- Name and contact details of the DPO (from where more information can be obtained).
- 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 delay⁵”*.

2.4.3. If the controller chooses to only notify the Data Protection Commission, it is recommended that the controller indicates, where appropriate, whether the breach involves establishments located in other Member States.

2.4.4. **Purpose of DPC notification:**

- (a) **Avoid an Administrative fine:** Failure to notify the Data Protection Commission as required under the Data Protection Act 2018 may result in an administrative fine.
- (b) **Advices:** so that the ETB can obtain advices from the DPC, and to ensure that the ETB’s decisions about notifying (or deciding not to notify) affected data subjects

⁴ Available at www.enisa.europa.eu/publications/dbn-severity

⁵ Article 33(4) GDPR.

can be justified.

2.4.5. Notifying affected data subjects

Following the risk-assessment conducted at 2.4.2, if the personal data breach is likely to result in a “high risk” to the rights and freedoms of natural persons, the ETB shall:

- (a) Contact the individuals concerned (whether by phone/email etc) without undue delay.
- (b) Advise that a data breach has occurred.
- (c) Provide the data subjects with the detail outlined at 2.5.2 above.
- (d) Where appropriate, provide specific advices so that the data subjects can protect themselves from possible adverse consequences of the breach (such as re-setting passwords).

2.4.6. The communication to the data subject shall not be required if any of the following conditions are met:

- (a) the ETB has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- (b) the ETB has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

2.4.7. An Garda Síochána:

- (a) Where data has otherwise been accessed without authority, the matter shall be reported immediately to An Garda Síochána.
- (b) Depending on the nature of the personal data at risk and particularly where sensitive personal data may be at risk, further assistance should be sought from An Garda Síochána.
- (c) 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.

2.4.8. Other bodies: Where appropriate, contact may be made with other bodies such as the HSE, TUSLA, financial institutions, ETBI etc. (depending upon the nature of the data put at risk, e.g. if it contains sensitive information relating to children or vulnerable persons, such as child protection or safeguarding matters).

2.4.9. Insurance company: DDLETB shall notify the insurance company with which the organisation is insured and advise them that there has been a personal data security breach.

2.5 ETB Legal Advisors, including as appropriate, the Legal Services Support Unit, Education and Training Boards’ Ireland: DDLETB may notify its legal advisors and advise them that there has been a personal data security breach for the purposes of obtaining legal advices and defending, compromising or otherwise settling litigation.

2.6 Post-event: After the initial response measures have been addressed, a full review should be undertaken in a timely manner. These should include the following:

- 2.6.1 Review of the breach record per Article 33(5) – document maintained by the ETB in its Risk Register.
- 2.6.2 Details of learning outcomes, improvements, and safeguards should be identified.
- 2.6.3 The ETB board shall receive an appropriate briefing from the DPO (and/or such other external experts as may be retained to assist), and a copy of any investigation reports and any correspondence exchanged with the DPC and/or affected data subjects.

- 2.6.4 The ETB will give careful consideration to whether disciplinary procedures should be initiated, if relevant.
- 2.6.5 Where remedial actions are necessary, responsibility shall be allocated to individual(s): they shall be allocated responsibility for ensuring certain actions are completed within defined timeframes.
- 2.6.6 Staff should be apprised of any changes to this protocol and of upgraded security measures. Staff should receive refresher training where necessary.

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: “<i>the information may be provided in phases without undue further delay</i>”⁶.

⁶ Article 33(4) GDPR.

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

**Have you spoken to someone in DDLETB Data Protection team at administrative head office level e.g. DPO at dataprotection@ddletb.ie ?
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 at dataprotection@ddletb.ie

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.

