

Business Unit:	Organisation Support & Development
Document Title:	Data Breach Protocol LWETB
Document No.	DP004/DB/V3/24

Longford and Westmeath Education and Training Board

Data Breach Protocol

1. Data breach and purpose of protocol

1.1. Longford and Westmeath Education Training Board (LWETB) has developed this personal data breach protocol to ensure that we are able to act promptly to protect individuals and their personal data. LWETB 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.

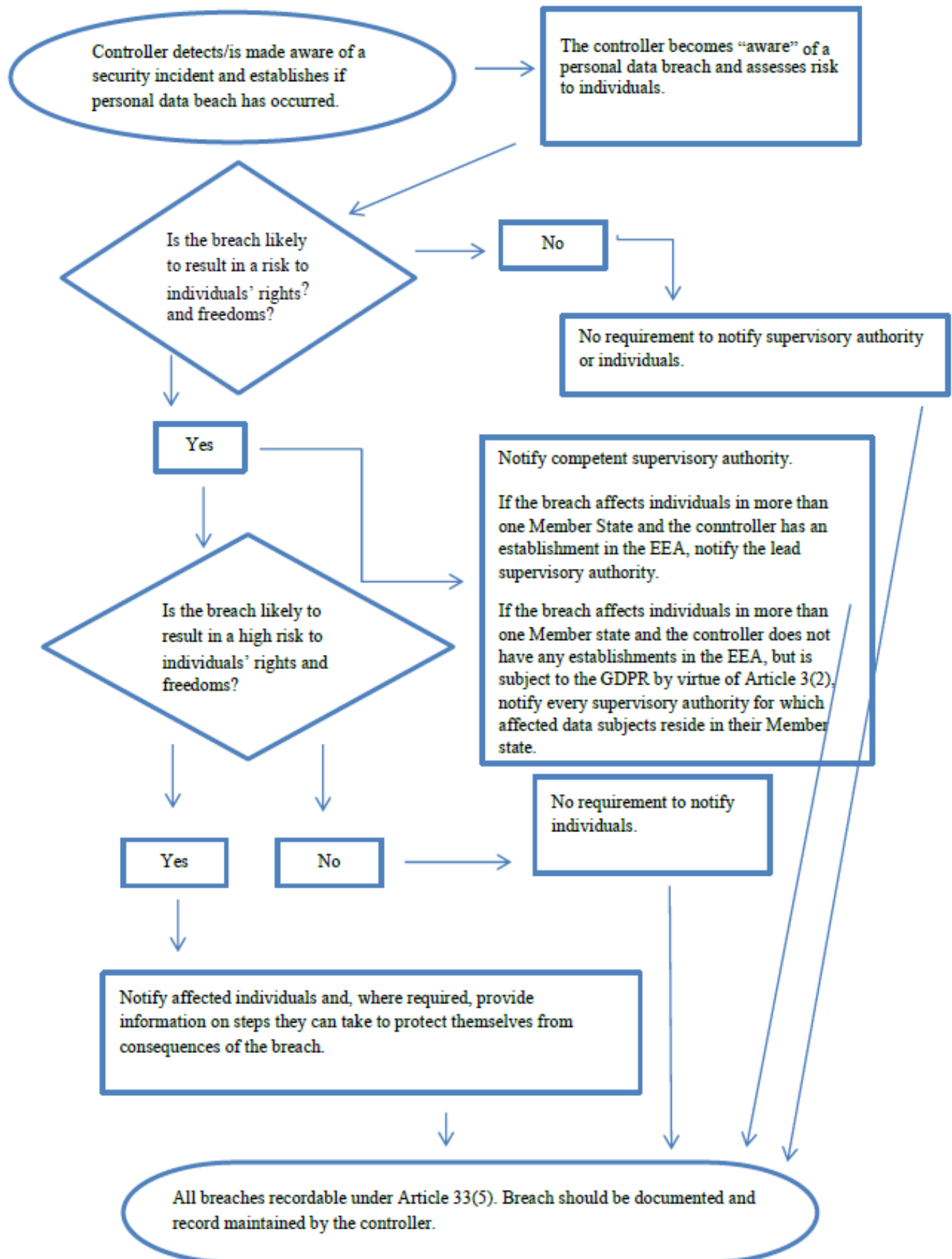
1.2. This protocol will be:

(a) circulated to all appropriate data processors. Data processors are required to alert LWETB immediately if the processor becomes aware of a breach of the personal data it is processing on behalf of LWETB

(b) advised to staff at induction and at periodic staff meetings/ training.

1.3. The following flow-chart (taken from the EDPB Guidelines 9/2022 on personal data breach notification under GDPR, Adopted on 28 March 2023) summarises the steps to be taken:

A. Flowchart showing notification requirements



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. **“Data Controller”**: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. LWETB is the data controller.
- 1.4.4. **“Data Processor”**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.
- 1.4.5. **“Data Subject”**: is an identified and identifiable natural person whose information is held by LWETB.
- 1.4.6. **“Destruction”**: the data no longer exists or no longer exist in a form that is of any use to the controller.
- 1.4.7. **“DPC”**: Data Protection Commission is the statutory body responsible for upholding the rights of individuals as set out in the Acts and enforcing the obligations upon data controllers.
- 1.4.8. **“DPO”**: Data Protection Officer, who is responsible for compliance with data protection regulations, monitoring specific processes, such as data protection impact assessments, employee awareness and training employees, as well as collaboration with authorities.
- 1.4.9. **“Loss”**: the data may still exist, but the controller has lost control of or access to the data, or no longer has the data in its possession.
- 1.4.10. **“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”.
- 1.4.11. **“Special Category data”**: information about somebody’s racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.
- 1.4.12. **“Temporary loss of data”**: an incident resulting in personal data being made unavailable for a period of time.
- 1.4.13. **“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.

1.5. 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 effects 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”*.

1.7. Personal data breaches can also be damaging to LWETB 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 LWETB.
- Damage to the reputation of LWETB.
- Administrative fines, enforcement action, and/or litigation in accordance with the provisions of Data Protection legislation.

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

² Page 8, WP250.

2. Protocol

In case of a personal data breach, LWETB will observe the following protocol:

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

2.1.1. The DPO (Data Protection Officer) shall be notified as soon as possible.

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

Emergency contact numbers:

Name of Data Protection Officer: Denis McDermott

Tel: 044 9348389

Mobile: 085 8621234

Email: dp@lwetb.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, 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/dataset 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 of having become aware of the breach.
- (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 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 Risk Register.

2.2. Containment, mitigation, and recovery

2.2.1. LWETB 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 LWETB. Their advice 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) ascertaining the nature of what personal data may potentially have been exposed.

2.2.4. LWETB will 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. LWETB 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? Classification of that risk:

- No risk?
- Risk?
- High risk?

If it is concluded that there is “no risk”, the reasons for that decision must be recorded.

2.3.2. When assessing risk, LWETB 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.

2.3.3. LWETB 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.

2.3.4. LWETB 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 breach³

2.3.5. 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 Risk Register.

2.4. Notification

2.4.1. **Reporting of incidents to the Data Protection Commission (“DPC”)**: All incidents in which 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 risk to the rights and freedoms of data subjects.

DPC Contact details

Telephone: 017650100
Lo Call Number: 1800437737
E-mail: info@dataprotection.ie
Address: Data Protection Commission,
21 Fitzwilliam Square South,
Dublin 2, D02 RD28, Ireland

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 whom 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 LWETB 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 delay⁴”*.

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

2.4.4 Purpose of DPC notification:

- (a) **Avoiding 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) **Advice:** so that LWETB can obtain advice from the DPC, and to ensure that LWETB's decisions about notifying (or deciding not to notify) affected data subjects can be justified.

2.4.5 Notifying affected data subjects

Following the risk-assessment conducted at 2.3 if the personal data breach is likely to result in a “high risk” to the rights and freedoms of natural persons, LWETB 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 2.4.2 above but taking care not to reveal any other data subjects' information to that person.
- (d) Where appropriate, provide specific advice 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) LWETB 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) LWETB 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 if the Breach Management Team decide it is warranted in the circumstances, and, in particular, by the risk assessment specified in section 2.3 above.
- (b) This will be determined on a case-by-case basis, and the reasons for reporting or not reporting will be fully documented.
- (c) 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.
- (d) 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: LWETB shall notify the insurance company with which the organisation is insured and advise them that there has been a personal data security breach.

IPB Insurance,
1 Grand Canal Square,
Grand Canal Harbour,
Dublin
D02 P820
01 639 5500
claims@ipb.ie

2.5 ETB Legal Advisors, including as appropriate, the Legal Services Support Unit, Education and Training Boards' Ireland: LWETB may contact its legal advisors and advise them that there has been a personal data security breach for the purposes of obtaining legal advice 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 LWETB in its Risk Register.
- 2.6.2 Details of learning outcomes, improvements, and safeguards should be identified.
- 2.6.3 The Board of LWETB 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 LWETB 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) 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.

³ Available at www.enisa.europa.eu/publications/dbn-severity

⁴ Article 33(4) GDPR.

Data Security Breach – Incident Report **CONFIDENTIAL**

On discovery of a data breach, please contact the DPO immediately, and then proceed to complete this report form.

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 LWETB 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”.

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

⁵Article 33(4) GDPR.


Have you spoken to someone in the ETB management team at administrative head office level? E.g. CE, Director, 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:	
Position:	
Contact number:	
Date:	
Time of completion:	

For Breach Management Team Use Only

Details logged by:	<i>Insert details in column below</i>
DPO Name:	
Date & Time report received:	
Type of personal data breach e.g. Confidentiality breach; integrity breach; availability breach (see Appendix 2 below)	
Numbers of likely people affected by the breach	<i>Estimated number of data subjects affected? Types of data affected?</i>
Were special categories (e.g. sensitive personal data) compromised in the breach? <i>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.</i>	Yes <input type="checkbox"/> No <input type="checkbox"/> <i>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?</i>
Severity of the breach <i>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.</i> Rate the breach in terms of its likely risk to 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 <input type="checkbox"/> No <input type="checkbox"/>
IT Service Providers / IT support to be notified	Yes <input type="checkbox"/> No <input type="checkbox"/>
Insurance Company to be notified	Yes <input type="checkbox"/> No <input type="checkbox"/>
Gardaí to be notified?	Yes <input type="checkbox"/> No <input type="checkbox"/>
Legal advisors to be notified? (including LSSU as determined by LWETB)	Yes <input type="checkbox"/> No <input type="checkbox"/>
Data Subjects to be notified? <i>How many?</i> <i>Is there a list of contact details for data subjects? If not, can we recover?</i>	Yes <input type="checkbox"/> No <input type="checkbox"/>
Data Protection Commission to be notified? Notification should be made by submitting a data breach report online at: https://forms.dataprotection.ie/breach-notification	Yes <input type="checkbox"/> No <input type="checkbox"/> <i>If YES, list date and time of notification and any advice/instruction given:</i>
Any additional relevant additional details	
Signed by DPO:	
Signed by CE / nominee:	
Date:	

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

Appendix 2 – General guidance on breach handling

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 access 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

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;
- Contact LWETB Data Protection Officer without delay;
- 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.

Appendix 3 - Guidelines on breach notification⁶ (for DPO only)

Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist DPO in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the DPC?	Notify the data subject?	Notes/recommendations
A staff member stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data is encrypted with a state of the art algorithm, backups of the data exist, the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However, if it is later compromised, notification is required.
A school offers an online enrolment facility. As a result of a cyber-attack, personal data of students is accessed.	Yes, if there are likely consequences to students.	Yes, report to students depending on the nature of the personal data affected and if the severity of the likely consequences to students is high.	
A brief power outage in the county means parents are unable to log on to VSware and access their children's records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the DPO.
A payroll department suffers a ransomware attack which results in all data being encrypted. No back-ups are available, and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes, if there are likely consequences to staff members as this is a loss of availability.	Yes, report to staff members, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there had been a backup available and data could have been restored in good time, this would not need to be reported to the DPC or to staff members as there would have been no permanent loss of availability or confidentiality. However, if the DPC became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32

⁶Extracted from: Article 29 Working Party 'Guidelines on Personal data breach notification under Regulation 2016/679'

<p>An adult learner phones a further education centre to report that he/she has received the exam results of somebody else.</p> <p>The DPO undertakes a short investigation (i.e. completed within 24 hours) and establishes with reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.</p>	<p>Yes.</p>	<p>Only the individuals affected are notified if there is high risk and it is clear that others were not affected.</p>	<p>If, after further investigation, it is identified that more individuals are affected, an update to the DPC must be made and the DPO takes the additional step of notifying other individuals if there is high risk to them.</p>
<p>A website hosting company acting as a data processor identifies an error in the code which controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.</p>	<p>The hosting company must notify its affected clients (the controllers) without undue delay. Assuming that the website hosting company has conducted its own investigation, the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having “become aware” once they have been notified by the hosting company (the processor). The controller then must notify the DPC.</p>	<p>If there is likely no high risk to the individuals, they do not need to be notified.</p>	<p>The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive as a digital service provider).</p> <p>If there is no evidence of this vulnerability being exploited with any of its controllers a notifiable breach may not have occurred, but it is likely to be recordable or be a matter of non-compliance under Article 32.</p>
<p>Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.</p>	<p>Yes, report to DPC.</p>	<p>Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.</p>	
<p>An e-mail is sent to recipients in the “to:” or “cc:” fields, thereby enabling each recipient to see the email address of other recipients.</p>	<p>Yes, potentially if a large number of individuals are affected, if sensitive data are revealed (e.g. a reminder email to parents re outstanding school charges)</p>	<p>Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.</p>	<p>Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.</p>