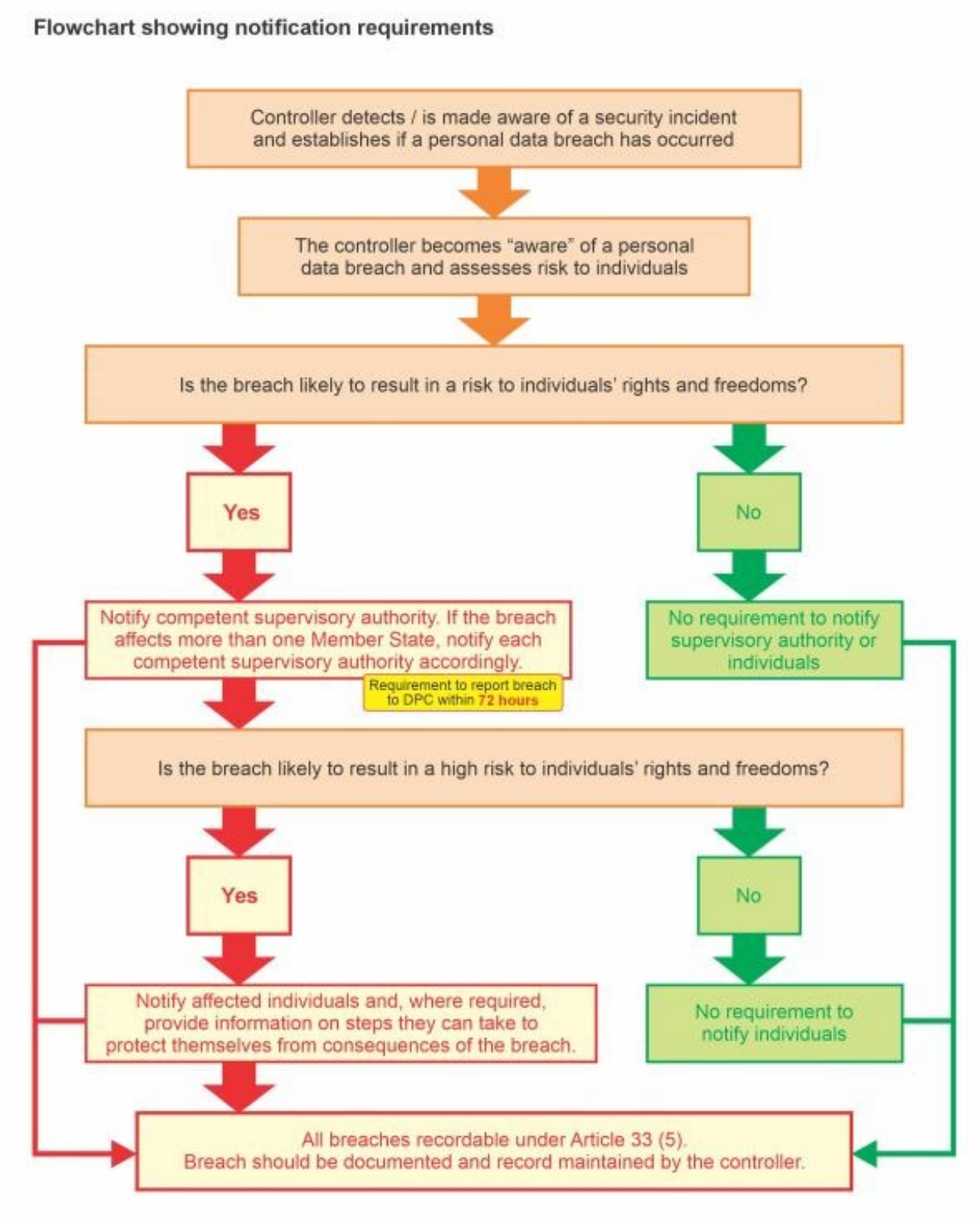
City of Dublin
Bord Oideachais agus Oiliúna
Education and Training Board

Data Breach

Staff Protocol

Version number	2.0
Guidance drafted by	ETBI Template modified by DPO
Approved by SLT on	28.04.2026
Next review date	2 years from approval

Contents



Note:

The competent 'supervisory authority' in Ireland is the Data Protection Commission (DPC).

NB. Any data breach that concerns the ETB's I.T. network infrastructure should also be immediately notified to the I.T. Department for guidance and further instruction.

1. Definitions:

In this, the following terms shall have the following meanings[1]:

1.1. "**aware**": a data controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that personal data has potentially been compromised.
1.2. "**damage**": the personal data has been altered, corrupted, or is no longer complete.
1.3. "**destruction**": the data no longer exists or no longer exists in a form that is of any use to the controller.
1.4. "**DPO**" Data Protection Officer, is a designated person who on behalf of City of Dublin ETB fulfils the tasks referred to in Article39 GDPR.
1.5. "**line manager**" is the person to whom you report to, such as a Principal, Deputy Principal, APO, AEO, Director, Centre Manager, Programme Coordinator
1.6. "**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.
1.7. "**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".
1.8. "**temporary loss of data**": an incident resulting in personal data being made unavailable for a period of time.
1.9. "**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 and data protection legislation.

2. Reasons for a personal data breach:

A personal data breach can happen for several reasons, for example:

- human error or intentional act,
- loss or theft of paperwork, or of any electronic device containing personal 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,
- any other information security breaches and/or errors

[1] Definitions taken from GDPR and Article 29 Data Protection Working Party 'Guidelines on Personal data breach notification under Regulation 2016/679'.

3. Effect of a personal data breach on individuals

Personal data breaches can have adverse effects on individuals which in turn may result in physical, material, or non-material damage. This could include causing the data subject embarrassment, distress, or humiliation. Examples of other adverse effects to affected individuals are:

- 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 disadvantage[2].

4. Effect of a personal data breach on City of Dublin ETB

Personal data breaches can also be damaging to City of Dublin ETB as they can result in:

- damage to the relationship of trust we have built with staff and students and other stakeholders,
- loss of, deletion of, or damage to personal data, which is essential to the administration of the ETB,
- damage to the reputation of City of Dublin ETB
- administrative sanctions and/or fines enforcement action from the Data Protection Commission, and/or litigation.

5. Procedure

In case of a personal data breach, City of Dublin ETB will follow this procedure:

2.1. If a staff member becomes aware of a possible breach of personal data, they must notify both their line manager and the City of Dublin ETB Data Protection Officer immediately. If the data breach involves any element of the I.T. infrastructure, then the I.T. Department must also be notified immediately.

1.1.1. City of Dublin ETBs DPO contact details are as follows: dataprotection@cdetb.ie / 087 750 3420

1.1.2. I.T. Department contact details are as follows – it@cdetb.ie

[2] Page 8, Data Protection Working Party 'Guidelines on Personal data breach notification under Regulation 2016/679'.

1.1.3. If the breach is caused by an email that has been sent in error, please endeavour to recall the said email without delay.

1.1.4. The staff member should record the sequence of events within the Data Breach Incident Report form (Appendix 1), including as much information as possible. The completed report should then be sent to dataprotection@cdetb.ie

1.1.5. All staff and all data processors and/or joint data controllers are required to give all necessary assistance to the DPO.

City of Dublin
Bord Oideachais agus Oiliúna
Education and Training Board

Data Security Breach – Incident Report

Confidential & Privileged

This form has been completed in contemplation of legal proceedings

The GDPR, in Article 4(12), defines a "*personal data breach*" 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*".

This form is to be completed by the person responsible for the breach, their line manager or the first person to become aware of it.

BREACH CHRONOLOGY & CONTACTS	
Unique Breach ID (office use only):	
When did the breach occur?	
Where did the breach occur?	
When was the breach discovered?	
Who discovered the breach?	
Contact details of breach reporter:	Name:
	Landline:
	Mobile:
	Email:
Was the DPO immediately notified? If **yes**, please indicate by what means (Phone/email *etc*.) and time and date of contact:	

If **no**, were any other senior officials (CE, Directors *etc*.) contacted and if so, please indicate by what means (Phone/email *etc*.) and time and date of contact:	Name:	
Were there any witnesses to this breach? If yes, please provide name/s and contact details:	Landline:	Name:
	Mobile:	Landline:
	Email:	Mobile:

BREACH DETAILS	
What was the nature of the breach? See 'For Reference' section below	
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 number *etc*.):	
Approximate numbers 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.):	
In your opinion, is the breach likely to be of a temporary nature?	
Can the personal information exposed be recovered?	
Have you taken any action/steps so far to stop/mitigate the risk either to the data subject/s who you think have been affected, or any additional data subjects you consider may be affected? If yes, please describe the actions taken:	

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, as per Article 33(4) of the GDPR: *"…the information may be provided in phases without undue further delay"*. ()

TECHNICAL DETAILS	
Was the breached data protected through passwords, encryption *etc*.? Please supply details.	
Were any IT systems involved? (*e.g.* email, website, school admin system, apps *etc*.). If so, please list.	
Is any additional material available? (*e.g.* error messages, screenshots, log files, CCTV footage *etc*.)	
If breach occurred through an IT system, what steps have been taken to contain the breach?	
What steps have been taken to prevent this occurrence from being repeated?	

COMMUNICATIONS	
Have you spoken to someone in the ETB Management Team at administrative head office level (*e.g*. Chief Executive, Director, Head of IT *etc*.)? If so, please advise whom you contacted, and a brief outline of the advice offered by them:	

ADDITIONAL INFORMATION
Please provide any further information that you think may be of relevance and that you have not already provided above:

FORM COMPLETION DETAILS
Name:
Mobile:
Landline:
Email:
School/Centre/Office:
Position:
Date of Form Completion:
Time of Form Completion:

Thank you for completing this form. This will assist us in investigating and analysing the situation. Please ensure that the completed form is forwarded directly to the Data Protection Officer at: aishling.lennon@cdetb.ie

For reference

Breaches can be categorised at:

- No Risk
- Low Risk
- Medium Risk
- High Risk
- Severe Risk

The Data Protection Team will review the Incident Report Breach Form and determine the category of breach.