Edmund Rice College

Carrigaline

Procedure for Handling a Personal Data Breach

March 2021

Ratified by the Board of Management on 9 March 2021

Procedure for Handling a Personal Data Breach

1. Scope and Purpose

1.1. The purpose of this procedure is to guide the school's response in the event of a personal data breach.[1]

1.2. This procedure will be:

(a) highlighted to staff at induction and at periodic staff meetings/ training.

(b) circulated to all appropriate data processors. Data processors are required to immediately contact the school should they become aware of a breach of personal data that is being processed by them on behalf of the school.

1.3. This procedure should be understood and applied in conjunction with other relevant school policies and procedures (most notably the school's Data Protection Policy).

1.4. The school's priority, in response to any personal data breach, will be to take prompt action to minimise any risk to individuals and their personal data.

1.5. In nearly all circumstances, an effective breach response by the school will require each of the areas of action (listed below) to be progressed in parallel with each of the others.[2]

- Confirm that a breach has occurred and investigate the facts surrounding it.
- Communicate as necessary with stakeholders, advisors and others.

[1] The data protection legislation changed on 25th May 2018 with the coming in to force of the GDPR and the imposition of a new set of legal obligations on data controllers including mandatory notification of data breaches in certain circumstances - as summarised in Appendix 3.

[2] The fact that these areas of action are presented sequentially in this procedure should not be taken to imply a sequential approach to managing a personal data breach.

- Implement actions to contain and mitigate the breach (including data retrieval where possible).
- Assess the extent of the risk to those affected and the likelihood of these risks materialising.
- Notify, as appropriate, the Data Protection Commission (DPC) and the affected data subjects.

2. Causes and Impact

2.1. **Causes** A personal data breach can come about as a consequence of either a deliberate action or an accident. And while the term 'data breach' is often used synonymously with 'cyber-attack', not all cyber-attacks result in data breaches, and it is certainly the case that not all data breaches are the result of cyber-attacks. In fact, most personal data breaches in schools (as elsewhere) occur as a consequence of human error. Common causes of data breaches include:

- Loss or inappropriate disposal of paperwork or any device containing data.
- Poor access controls allowing unauthorised use or access.
- Theft, burglary, mugging.
- 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.

2.2. **Effects of breaches on individuals** Personal data breaches can have adverse effects on individuals and lead to physical, material, and non-material damages. These can include causing embarrassment, distress, and/or humiliation. Other adverse effects to individuals may 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 disadvantage.*[3]

2.3. **Effects of breaches on the school** Personal data breaches can also be damaging to the school as they can result in:

- Damage to the relationship of trust built with stakeholders (students, parents, staff, trustees and members of wider community).
- Consumption of school resources in addressing investigation, mitigation, remediation and communication issues.
- Loss of, or damage to, personal data essential to the administration of the school.
- Administrative sanctions and fines in accordance with the provisions of Data Protection legislation.
- Exposure to potential litigation.

3. Definition and Investigation

3.1. **Definition of a personal data breach** A personal data breach is a breach that impacts on personal data (i.e. information that relates, directly or indirectly, to an identifiable person).[4] A personal data breach occurs whenever the confidentiality, availability or integrity of this type of information is compromised.

[3] Page 8, *Article 29 Working Party Guidelines on Personal Data Breach Notification under Regulation 2016/679 (WP250).*

[4] While data breaches can happen to any kind of information, GDPR is only concerned with personal data. GDPR 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*.

3.2. All staff should be able to recognise a personal data breach and understand that personal data doesn't need to have been disclosed to a third party; it may also have been altered, corrupted, lost or destroyed.[5]

3.3. The information received in the early stage of a breach of personal data is not always accurate or complete. Some degree of investigation may be needed to rapidly establish whether the integrity of personal data under the school's control has been compromised.

3.4. It may be appropriate to gather together a small team to assess any potential exposure/loss and identify appropriate containment/mitigation/remediation measures.[6]

3.5. The scope of any investigation should reflect the information requirements set out in the data protection legislation. GDPR Article 33(5) requires schools to document all personal data breaches (regardless of level of risk or impact). The "Data Security Breach Incident Report" form (Appendix 1) provides a suitable template.[7]

3.6. Any initial investigation of a data breach might focus on clarifying the following information:

(a) Date/time of initial communication of breach, including details of who reported the matter.
(b) Details of what is known/suspected at this initial stage.
(c) Details of what system/data is involved.
(d) Any tasks necessary to confirm the occurrence and extent of the breach.
(e) An initial assessment of any risks to the rights and freedoms of natural persons.
(f) List of potential follow-on actions (investigation, containment, mitigation, recovery, etc).
(g) Summary of tasks assigned to relevant staff and others (e.g. IT service providers etc).
(h) Details of all likely communications, including any notifications to DPC and affected individuals.

3.7. In appropriate circumstances, consideration may need to be given to retaining an IT forensics specialist.

4. Communications[8]

4.1. **Staff**

(a) All staff should understand the need to report a suspected breach to senior management in a timely manner. Early recognition and communication is essential if the 72 hour limit for notification to the DPC is be observed and the rights of data subjects are to be protected.

[5] The school should provide staff with access to relevant information and training as appropriate.

[6] All staff and all data processors and/or joint data controllers are required to give all necessary assistance to the Principal and this team.

[7] Regardless of whether (or not) a decision is made to notify the DPC, all documentation relating to a personal data breach, including but not limited to the documentation required by GDPR Article 33(5), should be stored in the school's GDPR Accountability file.

[8] Important Note: the school should avoid including any personal data in the documentation or information that is being shared as part of these communication processes. While the recipients will generally be bound by a duty of confidentiality, there is usually no purpose or

(b) All staff should be aware that the 72 hour time period does not differentiate between working and non-working days[9] and commences from the moment the data controller becomes aware of a data breach.[10]

4.2. **Board of Management** The Principal must report all personal data breaches to the Board of Management. [11] The Board should agree a clear protocol with the Principal around the timing of these communications. For example,

(a) for any data breaches that are assessed as "low risk", it might be agreed that these are routinely notified to the Board at its termly business meeting.

(b) for a breach assessed as "high risk", it might be agreed that the Principal would inform the Chairperson at the earliest opportunity.[12]

4.3. **An Garda Síochána**

(a) Depending on the nature of the personal data breach, and particularly where sensitive personal data may be at risk, assistance might be sought from An Garda Síochána.

(b) Where data has been accessed without authority, the matter shall be reported immediately to An Garda Síochána.[13]

(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.

4.4. **Insurance Company** Where there is deemed to be risk associated with a personal data breach then the school should contact its insurance company to advise them that there has been a security incident.

4.5. **Legal Advisors** The school may notify its legal advisors and advise them that there has been a security breach for the purposes of obtaining legal advices and defending, compromising or otherwise settling litigation.

4.6. **Others** Where appropriate (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) contact may be made with other bodies such as the HSE, TUSLA, financial institutions, etc.

---

benefit to sharing the actual personal data that has been breached. For example, the DPC generally advises that it does not want controllers to include any affected personal data when filing a mandatory breach notification. Similarly, while a school's Board of Management may choose to review a personal data breach in detail in order to fulfil its responsibilities as data controller, this function will rarely if ever require the Board to access the personal data itself.

[9] For example, if the school becomes aware of a data breach at 9am Friday, then a notification (if required) will need to be filed no later than Monday 9am.

[10] The school can be regarded as having become "aware" whenever there is a reasonable degree of certainty that a security incident has led to personal data being compromised.

[11] The Board of Management is the designated Data Controller and, as such, should have an understanding of the key data protection issues that relate to the school's operation. It is therefore recommended that "Data Protection" is included as a recurring item on the agenda of Board meetings. The fact that the incidence of data breaches must be communicated to the Board does not necessitate the sharing of any personal data with the Board as part of this reporting process.

[12] Early notification will allow the Chairperson to act in a timely action (e.g. to convene an emergency meeting of the Board where this is deemed necessary. In certain circumstances it may be appropriate to give consideration to the preparation of a press release.).

[13] "If you believe your account or your network has been hacked because you can't get access or you have noticed unusual activity, you should report it to your local Garda station". Garda Cybercrime advice https://www.garda.ie/en/Crime/Cyber-crime/ (accessed March 2020).

5. Containment and Recovery

5.1. The school will immediately seek to contain the incident (insofar as that is possible) and take all feasible steps to mitigate any further exposure or risk.

5.2. Depending on the nature of the breach/threat to personal data, appropriate containment actions may include:

- a quarantine of manual records storage area/s and other areas
- immediately retrieving paper documents from any unintended recipients
- directing staff not to access PCs, networks, devices etc.
- changing passwords for affected applications, devices, systems or rooms
- advising users to change their passwords
- acting to suspend user access and/or accounts
- an audit of records held on backup server(s)
- contacting any recipient of an email sent in error and asking them confirm deletion
- immediately disabling any lost or stolen electronic devices
- remotely locating, disabling and/or deleting data stored on a mobile device
- restoring a database or system from a back-up
- disabling network or system access
- notifying staff and/or Processors to do (or refrain from doing) something
- ensuring that actions don't inadvertently compromise the integrity of any investigation.

5.3. Where the security incident relates to an IT system and/or electronic data, timely contact may need to be made with the school's IT service providers(s) and their advices and assistance sought in relation to appropriate measures of containment, quarantine, preservation of data and logs[14] etc.

5.4. For serious incidents the school may seek input from an independent expert. Independent expertise can help to determine the source and scope of the breach, collect and analyse evidence, and outline remediation steps.

6. Risk Assessment

6.1. The school must undertake an assessment in relation to the risk(s) arising from any personal data breach i.e. is the personal data breach likely to result in a risk to the rights and freedoms of natural persons?[15]

6.2. In assessing the level of risk, the school must focus on the risk to the data subjects e.g.

(i) What are the potential adverse consequences for individuals? [16]

(ii) How serious are these consequences?

(iii) How likely is it that these consequences will materialise?

[14] IT logs and audit trails (e.g. firewall, router and intrusion detection systems) can be a particularly important source of forensic information following on a data security incident. The DPC may well enquire about these as part of its own review of a data breach incident.

[15] Although a personal data breach can present a source of risk to the school, the assessment required under GDPR Articles 33, 34 is exclusively concerned with any risk to the data subjects affected by the breach. The *European Union Agency for Network and Information Services* (ENISA) has published a methodology to help assess the severity of any breach, available at www.enisa.europa.eu/publications/dbn-severity

[16] The school must bear in mind that the potential impact of any data breach is not just loss of control over personal data. A breach can also result in other economic and social disadvantage including discrimination, identity theft, financial loss, damage to reputation, etc.

6.3. If the data breach concerns the data of children or other vulnerable individuals, then this will inevitably heighten the level of risk.

6.4. The risk assessment process must provide an outcome that allows the school to classify the level of risk associated with the breach, as either:

A. There is **no risk or any risk is unlikely to materialise**
B. There is **risk**
C. There is **high risk**.

This formal classification of the level of risk to the rights and freedoms of the data subjects is essential as it is a key determinant of how the school should manage the breach.

6.5. When managing a personal data breach, the school is advised to pay particular attention to relevant guidance issued on an ongoing basis by the *Data Protection Commission* (DPC). For example, the DPC has listed the following criteria as important when evaluating the risk to the rights and freedoms of affected data subjects:

- the nature and circumstances of the breach;
- the type of personal data affected (including whether it contains sensitive, or 'special category' personal data);
- the volume of personal data involved;
- the potential for the personal data to be used maliciously;
- the potential damage or harm to data subjects; and
- steps taken or the possibility to mitigate the harm or damage. [17]

6.6. The DPC refers data controllers to relevant guidance issued at a European level. For example, the European Data Protection Board (EDPB) recommends that any risk assessment should consider factors such as: [18]

- The type and circumstances of the breach (confidentiality/availability/integrity)
- Special characteristics of the individual (e.g. a breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result).
- The nature, sensitivity, and volume of personal data (e.g. breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if accessed together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data).
- Ease of identification of individuals (e.g. data protected by an appropriate level of pseudonymisation can reduce the likelihood of individuals being identified; encryption can make data unintelligible to unauthorised persons without the decryption key).
- Severity of consequences for individual (e.g. whether personal data is in the hands of people whose intentions are possibly malicious, or alternatively, sent in error to a recipient who can be trusted not to read or access, may be factored into the risk assessment the controller carries out following the breach. Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term).
- The number of affected individuals (Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data).

[17] See "Assessing Risk" in *A Practical Guide to Personal Data Breach Notification's under the GDPR* (DPC Guidance Note, October 2019). https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf

[18] *Guidelines on Personal Data Breach Notification Under Regulation 2016/679 (WP250).* *https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827*

6.7. Where the school forms the opinion that there is "no likely risk" to the rights and freedoms of the data subjects, the reasons for that decision must be recorded. The *Data Security Breach Incident Report* form (Appendix 1) provides a template. It is important that any decision that there is no necessity to communicate with the DPC and/or affected data subjects, is justified and documented within the records of the incident retained by the school, not least because this is a legal requirement under GDPR Article 33(5).[19]

7. Mandatory Notifications

7.1. **In the event of a personal data breach the school must** (inter alia):

i Notify the Data Protection Commission (DPC) without undue delay and not later than 72 hours unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

ii Contact the 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.

7.2. **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 risk to the rights and freedoms of data subjects.

7.3. While contact details for the Data Protection Commission are provided below, the recommended means of formally notifying a personal data breach to the DPC, is to use the breach notification form available on the Commission's website.[20] Completing and submitting the breach report webform will generate the necessary acknowledgment and DPC case reference number.

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, Portarlington, R32 AP23, Co. Laois

7.4. GDPR Article 33(3) requires that, at a minimum, the following information be provided to the DPC:

- ☐ nature of the personal data breach.
- ☐ categories (e.g. children, other vulnerable groups, people with disabilities, employees, customers) and 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 affected.
- ☐ likely consequences of the breach (e.g. loss of control of data, possible discrimination, identity theft, financial loss, physical risk etc).
- ☐ measures taken (or proposed) by the school to address the breach (including any measures to mitigate its possible adverse effects).
- ☐ Contact point for more information where appropriate

[19] "This means that the default position for controllers is that all data breaches should be notified to the DPC, except for those where the controller has assessed the breach as being unlikely to present any risk to individuals and the controller can show why they reached this conclusion. In any event, for all breaches — even those that are not notified to the DPC on the basis that they have been assessed as being unlikely to result in a risk — controllers must record at least the basic details of the breach, the assessment thereof, its effects, and the steps taken in response, as required by Article 33(5) GDPR." *Data Protection Commission 2019 Annual Report* p35.

[20] DPC Breach Notification Form https://forms.dataprotection.ie/report-a-breach-of-personal-data

7.5. 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".*

7.6. Purpose of DPC notification:

(a) Advices: so that the school can obtain advices from the DPC, and to ensure that the school's decisions about notifying (or deciding not to notify) affected data subjects can be justified.

(b) 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.

7.7. **Notifying affected data subjects** Following the risk-assessment exercise (section 6 of this procedure), if the personal data breach is deemed likely to result in a "high risk" to the rights and freedoms of natural persons, the school 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 7.8 below.

(d) Where appropriate, provide specific advices (such as re-setting passwords etc.) so that the data subjects can protect themselves from possible adverse consequences of the breach.

7.8. GDPR Article 34(2) requires that, at a minimum, the following information be provided to the Data Subjects

☐ Description of any likely consequences of the personal data breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy etc).
☐ Description of measures taken (or proposed) by the school to address the breach (including any measures to mitigate its possible adverse effects).
☐ Contact point for more information where appropriate

7.9. GDPR Article 34(3) states that a communication to the data subject shall not be required if any of the following conditions are met:

(a) the school has implemented appropriate technical and organisational protection measures, and those measures render the personal data unintelligible to any person who is not authorised to access it;

(b) the school 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.)

7.10. Where the DPC has reason to believe that the incident is being managed effectively by the school and that no further action is needed to protect individual rights and freedoms, this may result in the case being closed. On the other hand, the DPC also has the option (and in some circumstances a statutory obligation) to take further action in line with its powers under GDPR Article 58.[21]

7.11. In addition to any sanction it might apply to the school (as controller), the DPC also has the power to prosecute individuals when it believes they have committed offences under the Data Protection Act 2018, for example, where persons have knowingly or recklessly, disclosed personal data without the prior authority of the controller.[22]

[21] Under GDPR Article 58 the Data Protection Commission can, inter alia, (i) require the school to provide further information or to compile a detailed report (ii) carry out a data protection audit (iii) carry out an on-site examination of school systems and procedures (iv) issue warnings or reprimands (v) impose an administrative fine (as set out in GDPR Article 83).

[22] *Offences* are set out in the *Data Protection Act 2018, Chapter 7*

8. Evaluation and Response

8.1. In the aftermath of a data breach (or "near miss"), the school should carry out a post-incident review to ensure that the steps taken were appropriate and to identify any areas that need improvement or action.[23]

8.2. The extent of the post-incident review should be proportionate to the seriousness of the incident and the level of risk associated with any data breach.

8.3. A post-incident review may involve consideration of the following questions:

- What action needs to be taken to reduce the risk of future breaches and minimise their impact?
- Do policies, procedures or reporting lines need to be improved to increase the effectiveness of the school's response to a data breach?
- Are there weak points in security controls that need to be strengthened?
- Are people aware of, and adequately trained in, information security measures?
- Is additional investment required to reduce exposure and, if so, what are the resource implications?

8.4. As any data breach incident file approaches closure, the various consultation channels (as set out earlier in section 3 *Communications*) should be revisited to confirm that all appropriate actions have been taken. The school should also confirm that its records of the personal data breach are comprehensive and satisfy the regulatory requirements.[24]

8.5. In certain circumstances the school may need to consider initiating action under the appropriate school disciplinary procedure.[25]

[23] "Businesses and organisations in control of personal data have an obligation to mitigate against all potential future breaches. The DPC has observed an increase in the number of repeat breaches of a similar nature by a large number of companies. …..Data controllers can take simple steps to attempt to mitigate these risks such as running staff training and awareness programs; implementing stringent password policies and multifactor authentication for remote access; habitually updating anti-virus and anti-malware software; ensuring that email and web filtering environments are correctly configured; and, ensuring that all computer devices are regularly updated with manufacturers' software and security patches." *Data Protection Commission 2019 Annual Report* p35.

[24] GDPR Article 33(5): "The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken."

[25] For example, disciplinary action may be required where an employee has received adequate training and guidance on data processing and security measures and ought reasonably to have been aware of the consequences for acting in a manner contrary to school policy and procedures. Similarly, a student who causes a personal data breach by acting in a manner that is at variance with the school's policies may also anticipate a proportionate sanction under the Code of Behaviour.

Appendix 1 - Data Security Breach Incident Report

1 Breach Timeline

Breach Timeline	
Do you know when the breach initially occurred?	
When was incident discovered (specific time and date) and who reported the breach (data subject/employee/third party etc)?	
When did senior management become aware?	

2 About the Breach

Description of how the breach occurred:[26]
How would you categorise this breach?
(i) Impact on Data? (e.g. Destruction/Loss/Alteration/Disclosure/Access/ Unavailability) (ii) Nature of breach? (e.g. Device/Paper Lost/Stolen/Inappropriate disposal/ Cyber-incident/ Unintended sharing/ Network security compromised etc.) (iii) Cause? (e.g. Employee/Contractor/External error/omission/intentional act etc.)

[26] 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".

3 About the Breached Data

What categories of data subjects (e.g. students or other vulnerable groups, adult learners, parents/guardians, employees, board members, others etc.) were affected and/or potentially affected by the breach?
Number of data subjects affected (actual/approximate/unknown)?
What identifying details (e.g. Name/DOB/Address/PPSN/Contact details/passport/Economic or Financial data/ Location data/Other) relating to individuals were disclosed?
Were any special categories of data involved (racial or ethnic origin, Political opinions, Trade Union membership, Sex life data, Health data, Genetic data, Biometric data, Religious or philosophical beliefs)?
Number of data records affected (actual/approximate/unknown)?

4 Measures in place before the Breach and measures to respond to the Breach

Describe any relevant security/organisational measures in place prior to the breach (passwords, encryption etc.) Have any deficiencies in these organisational or technical measures been identified as a result of this breach?

Have any actions/steps been taken to mitigate the risk to the data subject(s)? Describe measures taken (or proposed) by the school to address the breach. Can the personal information be recovered?
Have you made any contact with external agencies e.g. Insurance Company, Gardaí, Legal advisors etc.? If YES, provide contact details and any advice provided.
Were any IT systems involved (e.g. email, website, MIS, apps)? Has any advice been obtained from IT provider/support? Is any additional diagnostic material available e.g. error messages, screen shots, log files, etc.?

5 Consequences and Notifications

Potential consequences of the breach for individuals (e.g. loss of control over data, discrimination, identity theft, financial loss, reputational damage etc)
How severe is the breach for affected individuals? Level of risk? None/Low/Medium/High/Severe. Note: Where you determine there is no risk, record how this was decided (including any consultation with Board).
Details of any contact with the DPC, including any formal breach notification(s) made in relation to this breach. (Copies of formal breach notifications can be appended to this form).
Details of any contact made with data subjects, including any written communications(s) made in relation to this breach. Copies of formal written communications(s) can be appended to this form.

Signed:	
Your position in the school:	
Date(s) of completion:	

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

Appendix 2 - Sources of Guidance on Data Security

The legal obligation to keep personal data secure applies to every data controller and data processor, regardless of size. The Data Protection Act 2018 and the General Data Protection Regulation (GDPR) do not detail specific security measures that a data controller or data processor must have in place. The absence of detail on security measures within the legislation should be understood on the basis that the provision of such guidance within the legislation would run the risk of going out of date quite quickly due to changes in technology etc.

At the same time, the GDPR, in Articles 25 and 32, does place an obligation on controllers and processors to implement data protection by design and by default and 'appropriate technical and organisational measures' to ensure a level of security appropriate to the risk, taking into account:

- the state of the art;
- the costs of implementation;
- the nature, scope, context and purposes of processing; and
- the likelihood and severity of the risk to the rights and freedoms of individuals.

It goes on to suggest the following indicative list of appropriate measures:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effective of technical and organisational measures for ensuring the security of the processing.

Data controllers and data processors are also obliged to ensure that their staff and other persons at the place of work are aware of security measures and comply with them.

DATA PROTECTION COMMISSION (DPC)

The DPC publishes guidance from time to time related to data security matters. This guidance, though technical in nature, is usually accessible to a broad audience in that it is written with the general reader in mind. Schools are advised to monitor the DPC website (www.dataprotection.ie) for relevant advice and to consider how it might apply within the school environment. Some examples of DPC guidance are listed below.

Guidance for Controllers on Data Security (updated February 2020)[27]

A set of general guidelines (12 pages) providing concrete advice for controllers in relation to issues such as:[28]

- Access Controls
- Access Authentication (Passwords and Multi-Factor Authentication)
- Automatic Screen Savers
- Encryption
- Anti-Virus Software
- Firewalls
- Software Patching
- Remote Access

[27] https://dataprotection.ie/en/guidance-landing/guidance-controllers-data-security

[28] In the event of a data breach it seems reasonable to anticipate that the DPC may use a controller's compliance with its own guidance on data security as an indicator of "appropriate technical and organisation measures". Bearing this in mind, it would seem appropriate for school data controllers to carefully review this guidance document (and any other relevant advice from the DPC). As part of any internal review of data security measures, the school might ask their nominated IT service providers to validate that they have implemented systems that are aligned with this DPC advice.

- Wireless Networks
- Portable Devices
- Logs and Audit Trails
- Back-Up Systems
- Incident Response Plans
- Disposal of Equipment
- Physical Security
- The Human Factor
- Certification

Guidance for Organisations on Phishing and Social Engineering Attacks (October 2019)[29]

This guidance (6 pages) provides controllers with tips on how to spot phishing and social engineering attacks, suggested approaches to mitigating risk, and a list of recommendations on how to increase organisational security.

- Tips to spot phishing or social engineering
- Approaches to mitigating the risk of attacks
- Recommendations to increase security against attacks

Guidance Note: What should you be aware of online? Some common online risks (October 2019)[30]

Familiarity with this guidance (22 pages) will benefit both the individual and the organisation. It aims to build user awareness of online risks and suggest steps "to keep yourself and your personal data safe and to exercise choice and control in deciding how you engage online with social media and other online services". The second part of the guidance highlights a number of security-related issues, including:

- Password Reuse
- Security Questions
- Phishing
- Unsecured Login Forms
- Domain Names – Spot Fake Sites

Guidance Note: Five Steps to Secure Cloud-based Environments (June 2019)[31]

Cloud-based environments offer many advantages; however, they also introduce a number of technical security risks which organisations should be aware of, including data breaches, hijacking of accounts, and unauthorised access to personal data. This DPC guidance (3 pages) aims to assist organisations understand their obligations with regard to the security of personal data, and to mitigate their risks when utilising a cloud-based environment.

Guidance Note: General Portable Storage Device Recommendations (October 2019)[32]

Any organisation utilising portable storage devices to store or transmit personal data should consider the particular risks associated with the use of such devices, such as loss or unauthorised access, and ensure that they have internal policies and technical measures which mitigate these risks. This guidance (3 pages) sets out recommendations for organisations to consider when planning their own internal policies on the use of portable storage devices.

[29] https://dataprotection.ie/en/guidance-landing/guidance-organisations-phishing-and-social-engineering-attacks

[30] https://dataprotection.ie/en/guidance-landing/common-online-risks

[31] https://dataprotection.ie/en/guidance-landing/five-steps-secure-cloud-based-environments

[32] https://www.dataprotection.ie/en/guidance-landing/general-portable-storage-device-recommendations

Data Security Guidance for Microenterprises (July 2019)[33]

This guidance (10 pages) is targeted at microenterprises but as most of its recommendations are equally applicable to an educational setting, it will be equally useful for schools engaged in a review of appropriate technical and organisational security measures to safeguard the personal data they are processing. As well as addressing technical security, it also provides very useful checklists on physical security and organisational security.

OTHER SOURCES

The **National Cyber Security Centre (Ireland)** was established a lead in the management of major cyber security incidents across government, and also to provide guidance and advice to citizens and businesses on major cyber security incidents. It has published a guide to cyber security for Irish business: *12 Steps to Cyber Security (October 2018)*.[34]

The **National Cyber Security Centre (UK)** has an extensive set of cybersecurity-related resources available on its website. These include support materials for public sector bodies[35] as well as specific guidance for school staff.[36] Those responsible for overseeing data security in schools may also find other NCSC resources to be of benefit, for example, its *Cyber Security: Small Business Guide*.[37]

ENISA, the European Union Agency for Cybersecurity, frequently publishes up to date guidance on cybersecurity, data protection and risk assessment available through its website.[38] For example, its *Guidelines for SMEs on the security of personal data processing*[39] explain how to implement a risk-based approach to data security. **Europol**, the European Union's law enforcement agency, also maintains some information relating to cybercrime on its website.[40]

Professional Development Service for Teachers (PDST), a national support service operating under the aegis of the Department of Education and Skills, supports the integration of ICT in teaching and learning within Irish primary and secondary schools. Where PDST shares guidance on IT security for schools this is likely to be available on the PDST Technology in Education website.[41]

[33] https://www.dataprotection.ie/en/guidance-landing/data-security-guidance-microenterprises

[34] https://www.ncsc.gov.ie/pdfs/Cybersecurity_12_steps.pdf

[35] https://www.ncsc.gov.uk/section/information-for/public-sector

[36] https://www.ncsc.gov.uk/information/resources-for-schools

[37] https://www.ncsc.gov.uk/files/cyber_security_small_business_guide_1.3..pdf

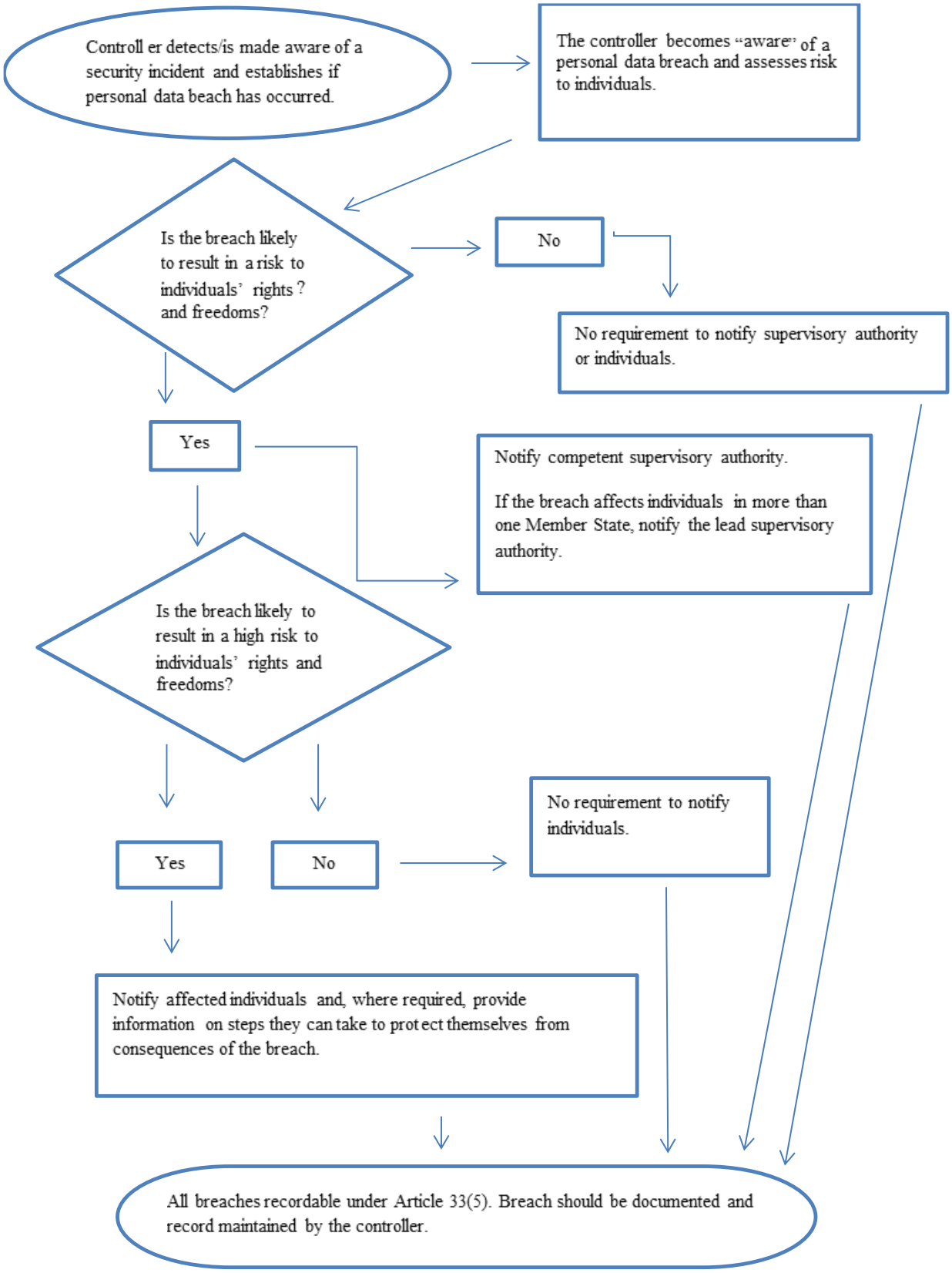
[38] https://www.enisa.europa.eu/topics

[39] https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

[40] https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

[41] https://www.pdsttechnologyineducation.ie/en/Technology/itsecurity/IT-Security.html

Appendix 3 - Flowchart showing regulatory notification requirements[42]



[42] This flowchart formed part of the *Guidelines on Personal data breach notification under Regulation 2016/679* adopted in 2018 by the **Article 29 Data Protection Working Party**, a body now reconstituted as the **European Data Protection Board**. https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827