Personal Data Security Breach Code of Practice

Date: September 2017

Purpose of Code of Practice

This Code of Practice applies to *Dublin and Dún Laoghaire ETB* as *data controller [1]*. This Code of Practice will be:

1. available on the school/centre website
2. circulated to all appropriate *data processors* and incorporated as part of the service-level agreement/data processing agreement between the school/centre and the contracted company and
3. shall be advised to staff at induction and at periodic staff meeting(s) or training organised by the school/centre.

Obligations under Data Protection

Dublin & Dún Laoghaire ETB as data controller and appropriate data processors so contracted, are subject to the provisions of the Data Protection Acts, 1988 and 2003 and exercise due care and attention in collecting, processing and storing personal data and sensitive personal data provided by data subjects for defined use.

Dublin & Dún Laoghaire ETB has prepared a **Data Protection Policy** and monitors the implementation of this policy at regular intervals. Dublin & Dún Laoghaire ETB retains records (both electronic and manual) concerning personal data in line with its **Data Protection Policy** and seeks to prioritise the safety of personal data and particularly sensitive personal data, so that any risk of unauthorized disclosure, loss or alteration of personal data is avoided.

Protocol for action in the event of breach

In circumstances where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the school/centre will follow the following protocol**:**

1. The school/centre will seek to contain the matter and mitigate any further exposure of the personal data held. Depending on the nature of the threat to the personal data, this may involve a quarantine of some or all PCs, networks etc. and requesting that staff do not access PCs, networks etc. Similarly, it may involve a quarantine of manual records storage area/s and other areas as may be appropriate. By way of a preliminary step, an audit of the records held or

[1] Unless otherwise indicated, terms used in this Code – such as “personal data”, “sensitive personal data”, “data controller”, “data processor” – have the same meaning as in the Data Protection Acts, 1988 and 2003.

backup server/s should be undertaken to ascertain the nature of what personal data may potentially have been exposed.

2. 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.

3. Where the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the school/centre may conclude that there is no risk to the data and therefore no need to inform data subjects or contact the Office of the Data Protection Commissioner. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

4. Depending on the nature of the personal data at risk and particularly where sensitive personal data may be at risk, the assistance of An Garda Síochána should be immediately sought. This is separate from the statutory obligation to report criminal damage to data arising under section 19 Criminal Justice Act 2011 as discussed at (2) above.

5. Contact should be immediately made with the data processor responsible for IT support in the school/centre.

6. In addition, and where appropriate, contact may be made with other bodies such as the HSE, financial institutions etc.

7. Reporting of incidents to the Office of Data Protection Commissioner: All incidents in which personal data (and sensitive personal data) has been put at risk shall be reported to the Office of the Data Protection Commissioner as soon as the school/centre becomes aware of the incident (or within 2 working days thereafter), save in the following circumstances:

    - When the full extent and consequences of the incident have been reported without delay directly to the affected data subject(s) **and**
    - The suspected breach affects no more than 100 data subjects **and**
    - It does not include sensitive personal data or personal data of a financial nature [2].

   Where all three criteria are not satisfied, the school/centre shall report the incident **via DDLETB, Data Protection Officer, Corporate Services Department** to the Office of the Data Protection Commissioner within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident (see further details below). Where no notification is made to the Office of the Data Protection Commissioner, the school/centre shall keep a summary record of the incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record shall comprise a brief description of the nature of the

[2] 'personal data of a financial nature' means an individual's last name, or any other information from which an individual's last name can reasonably be identified, in combination with that individual's account number, credit or debit card number.

incident and an explanation why the school/centre did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records shall be provided to the Office of the Data Protection Commissioner upon request.

8. The school/centre shall gather a small team of persons together to assess the potential exposure/loss. This team will assist the principal/manager of the school/centre (and DDLETB's DP Compliance Officer) with the practical matters associated with this protocol. The CEO of DDLETB should also be contacted and action undertaken in accordance with the CEO's direction/advice.

9. The team will, under the direction of the principal/manager, give immediate consideration to informing those affected [3]. At the direction of the principal (and/or CEO of DDLETB), the team shall:
    - Contact the individuals concerned (whether by phone/email etc.) to advise that an unauthorised disclosure/loss/destruction or alteration of the individual's personal data has occurred.
    - Where possible and as soon as is feasible, the *data subjects* (i.e. individuals whom the data is about) should be advised of
        - the nature of the data that has been potentially exposed/compromised;
        - the level of sensitivity of this data and
        - an outline of the steps the school/centre intends to take by way of containment or remediation.
    - Individuals should be advised as to whether the school/centre intends to contact other organisations and/or the Office of the Data Protection Commissioner.
    - Where individuals express a particular concern with respect to the threat to their personal data, this should be advised back to the principal/manager who may, advise the relevant authority e.g. Gardaí, HSE etc.
    - Where the data breach has caused the data to be "damaged" (e.g. as a result of hacking), the CEO of the ETB shall contact An Garda Síochána and make a report pursuant to section 19 Criminal Justice Act 2011.
    - The CEO of the ETB shall notify the insurance company which the school/centre is insured and advise them that there has been a personal data security breach.

10. Contracted companies operating as data processors: Where an organisation contracted and operating as a *data processor* on behalf of DDLETB becomes aware of a risk to personal/sensitive personal data, the organisation will report this directly to the school/centre as a matter of urgent priority. In such circumstances, the principal of the school/centre should be contacted directly (and in the case of an ETB school/centre, both the principal/manager and the Chief Executive Officer

---

[3] Except where law enforcement agencies have requested a delay for investigative purposes. Even in such circumstances consideration should be given to informing affected data subjects as soon as the progress of the investigation allows. Where DDLETB receives such a direction from law enforcement agencies, they should make careful notes of the advice they receive (including the date and the time of the conversation and the name and rank of the person to whom they spoke). Where possible, DDLETB should ask for the directions to be given to them in writing on letter-headed notepaper from the law enforcement agency (eg. An Garda Siochána), or where this is not possible, DDLETB should write to the relevant law enforcement agency to the effect that "we note your instructions given to us by your officer [insert officer's name] on XX day of XX at XXpm that we were to delay for a period of XXX/until further notified by you that we are permitted to inform those affected by the data breach."

should be contacted). This requirement should be clearly set out in the data processing agreement/contract in the appropriate data protection section in the agreement.

11. A full review should be undertaken using the template Compliance Checklist and having regard to information ascertained deriving from the experience of the data protection breach. Staff should be apprised of any changes to the Personal Data Security Breach Code of Practice and of upgraded security measures. Staff should receive refresher training where necessary.

Further advice: What may happen arising from a report to the Office of Data Protection Commissioner?

- Where any doubt may arise as to the adequacy of technological risk-mitigation measures (including encryption), the school/centre shall report the incident to the Office of the Data Protection Commissioner within **two working days** of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact will be by e-mail, telephone or fax and shall **not** involve the communication of personal data.
- The Office of the Data Protection Commissioner will advise the school/centre of whether there is a need for the school/centre to compile a detailed report and/or for the Office of the Data Protection Commissioner to carry out a subsequent investigation, based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.
- Should the Office of the Data Protection Commissioner request the school/centre to provide a detailed written report into the incident, the Office of the Data Protection Commissioner will specify a timeframe for the delivery of the report into the incident and the information required. Such a report should reflect careful consideration of the following elements:

    - the amount and nature of the personal data that has been compromised
    - the action being taken to secure and/or recover the personal data that has been compromised
    - the action being taken to inform those affected by the incident or reasons for the decision not to do so
    - the action being taken to limit damage or distress to those affected by the incident
    - a chronology of the events leading up to the loss of control of the personal data; and
    - the measures being taken to prevent repetition of the incident.

Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where the school/centre has not already done so. If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.