St Brigid's GNS, Palmerstown, Dublin 20.

Personal Data Security Breach Code of Practice

Purpose of Code of Practice
This Code of Practice applies to *St Brigid's GNS* as *data controller[1]*. This Code of Practice will be:

1. available on the school website
2. circulated to all appropriate *data processors* and incorporated as part of the service-level agreement/data processing agreement between the school 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.

Obligations under Data Protection
The school as data controller and appropriate data processors so contracted, are subject to the provisions of the Data Protection Acts, 1988 to 2018 and Regulation (EU) 2016/679 of the European Parliament and of the Council (i.e. General Data Protection Regulation – GDPR) and exercise due care and attention in collecting, processing and storing personal data and sensitive personal data provided by data subjects for defined use.

The school has prepared a **Data Protection Policy** and monitors the implementation of this policy at regular intervals. The school 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 will adhere to the following protocol**:**

1. The school 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,

[1] Unless otherwise indicated, terms used in this Code – such as "personal data", "data controller", "data processor" – have the same meaning as in the Data Protection Acts, 1988 and 2003 and GDPR. "Sensitive Personal Data" includes, in addition to sensitive personal data as defined in the Data Protection (Amendment) Act 2003, that data referred to in GDPR as "Special Categories of Personal Data"

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

2. The school as data controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of a personal data breach, notify such breach to the Office of the Data Protection Commissioner.
3. Where the notification to the Office of the Data Protection Commissioner is not made within 72 hours, it shall be accompanied by reasons for the delay.
4. Any third party processor shall notify the school (controller) without undue delay after becoming aware of a personal data breach. In accordance withy clause 16 below
5. The notification referred to in paragraph 2 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
   (b) communicate the name and contact details of the data protection officer or other contact person where more information can be obtained
   (c) describe the likely consequences of the personal data breach;
   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
6. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
7. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Data Protection Commissioner to verify compliance with domestic legislation and Article 33 of GDPR.
8. The school 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 backup server/s should be undertaken to ascertain the nature of what personal data may potentially have been exposed.
9. Where data has been "damaged" (as defined in the Criminal Justice Act 1991, e.g. as a result of hacking), the matter must also 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.

9. Where the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, by virtue of being protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the school may conclude, as provided in Article 33 of GDPR, 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.

10. 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 referred to above.

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

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

13. The school shall gather a small team of persons together to assess the potential exposure/loss. This team will assist the principal of the school (and the school's DP Compliance Officer) with the practical matters associated with this protocol.

14. The team will, under the direction of the principal, give immediate consideration to informing those affected in compliance with Article 34 of GDPR At the direction of the principal, the team shall:
    - When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the personal data breach shall be communicated to the data subject without undue delay (whether by phone/email etc.) to advise that an unauthorised disclosure/loss/destruction or alteration of the individual's personal data has occurred.
    - The communication to the data subject referred to above shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of clause 5 above.
    - Individuals should be advised as to whether the school 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 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 principal shall contact An Garda Síochána and make a report pursuant to section 19 Criminal Justice Act 2011.
    - The principal shall notify the insurance company which the school is insured and advise them that there has been a personal data security breach.
15. The communication to the data subject referred to in paragraph 14 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 were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption

    (b) the controller 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

16. Where an organisation contracted and operating as a *data processor* on behalf of the school becomes aware of a risk to personal/sensitive personal data, the organisation will report this directly to the school as a matter of urgent priority. In such circumstances, the principal of the school should be contacted directly, this requirement should be clearly set out in the data processing agreement/contract in the appropriate data protection section in the agreement.
17. A full review should be undertaken using the DPC Compliance Checklist template, 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 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 of whether there is a need for the school 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 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 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.

Ratified by the Board of Management on the 17th January 2019.