St Mary's Christian Brothers' Grammar School

Personal Data Breach Management Procedure

June 2018

EXECUTIVE STATEMENT

St. Mary's CBGS collects, holds, processes and shares large amounts of personal data, a valuable asset that needs to be suitably protected. Every care is taken to protect personal data and to avoid a data protection breach, however, in such circumstances, it is vital that immediate action is taken to contain and remedy the breach.

The Data Protection Officer (DPO) is legally required to notify the Information Commissioner's Office (ICO) of any personal data breach within 72 hours of becoming aware of it therefore it is essential that immediate action is taken by the School when a breach has occurred or is likely to occur. Individuals affected by the personal data breach must also be notified promptly.

Following the containment and remedy stage, steps must be taken to assess and determine the cause of the breach to ensure processes are reviewed and risk is minimised going forward.

This Data Breach Management Procedure (the Procedure) provides guidance for school staff members on how a Personal Data Breach should be handled and is intended for internal use.

It places obligations on staff to report actual or suspected personal data breaches and sets out the steps to be followed by the School for managing and recording actual or suspected breaches. The Procedure applies to all personal data held and processed by the School regardless of format.

1. Scope

1.1 The aim of this Procedure is to standardise the response to all reported data breach incidents, and ensure that they are appropriately logged and managed in accordance with best practice guidelines.

1.2 By adopting a standardised, consistent approach to all reported incidents it aims to ensure that:

1.2.1 immediate action is taken;

1.2.2 incidents are handled by appropriately authorised and skilled personnel;

1.2.3 incidents are recorded and documented;

1.2.4 the impact of the incidents are understood and action is taken to prevent further damage;

1.2.5 external bodies or Data Subjects (defined below) are informed as required;

1.2.6 incidents are dealt with in a timely manner and normal operations restored;

1.2.7 evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny; and

1.2.8 incidents are reviewed to identify improvements in policies and procedures.

1.3 The following terminology is used in this Procedure:

Term	Meaning
Data Protection Officer or DPO	The person we appoint from time to time to be involved in all aspects of the development and implementation of our data protection and data privacy strategy and compliance with the GDPR and other applicable laws.
Data Subject	The individual to whom the personal data relates.
GDPR	The General Data Protection Regulation.
Personal Data	Information relating to an individual who can be identified (directly or indirectly) from that information.
Personal Data Breach	Any incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, e.g. accidental loss, destruction, theft, corruption or unauthorised disclosure of Personal Data.
Special Category Data	Personal Data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

2. What is a Personal Data Breach?

2.1 A Personal Data Breach causes, or has the potential to cause, damage to the School's information assets, its reputation or to a Data Subject. A personal data breach may be recent, or historical and only just discovered.

2.2 Examples of a Personal Data Breach include but are not restricted to, the following:

2.2.1 loss or theft of Personal Data or equipment on which Personal Data is stored (e.g. loss of laptop, USB pen, iPad/tablet device, hard copy file or paper record);

2.2.2 alteration of personal data without permission or authorisation;

2.2.3 unauthorised disclosure of Personal Data;

2.2.4 sending Personal Data to the wrong recipient;

2.2.5 attempts (failed or successful) to gain unauthorised access to information or IT systems;

2.2.6 loss of availability of Personal Data (e.g. hacking attacks);

2.2.7 'blagging' offences where information is obtained by deceiving the organisation who holds it;

2.2.8 human error;

2.2.9 an identified vulnerability or weakness which may lead to a Personal Data breach.

3. Who is responsible under this Procedure?

3.1 **All staff, workers, contractors or volunteers employed or otherwise engaged at the School** must report any actual, suspected, threatened or potential Personal Data Breach and assist with investigations as required, particularly if urgent action is required to prevent further damage.

3.2 **Teachers** are responsible for overseeing the implementation of recommendations resulting from a Personal Data Breach so far as possible within their control.

3.3 **The Principal** must ensure that all staff, workers, contractors and volunteers comply with this Procedure, assist with investigations and implement improvement measures. The Principal is also the primary point of contact within the School for any data protection issues and is the interface with the School's DPO. The Principal will work closely with the DPO in relation to any actual, suspected, threatened or potential Personal Data Breach.

The Data Protection Officer (DPO) is responsible for supporting the Principal in managing a Personal Data Breach in accordance with this Procedure and will be the point of contact with the ICO. In our case, the Education Authority is our DPO and contact details are as follows:

Education Authority
40 Academy Street
Belfast
BT1 2NQ

Email: dpo@eani.org.uk

4. Reporting a Personal Data Breach

4.1 Anyone discovering an actual, suspected, threatened or potential Personal Data Breach must report it immediately to the Principal as the primary point of contact.

4.2 The Principal must then immediately and in any event within one hour report the Personal Data Breach to the DPO at dpo@eani.org.uk using the Data Breach Report Form set out in **Appendix 1** (where possible) followed up immediately by a phone call to 028 8241 1300Any actual, suspected, threatened or potential Personal Data Breach discovered outside of normal working hours must be reported by calling the Principal on:

Email: info@stmarys.belfast.ni.sch.uk

St. Mary's CBGS

147a Glen Road
BELFAST
BT11 8NR
02890294000

4.3 The Principal's report to the DPO should include full and accurate details of the incident including who is reporting the incident and what Personal Data is involved.

4.4 When a data breach has been reported to the DPO, the incident will be logged on a central system to facilitate effective management of the breach and to aid reporting.

4.5 All staff should be aware that any Personal Data Breach by them or any failure to report a Personal Data Breach in accordance with this **paragraph 4** may result in the matter being considered under the relevant disciplinary procedure.

5. Dealing with a Personal Data Breach

5.1 There is no single method of response to a Personal Data Breach. Incidents must be dealt with on a case by case basis.

5.2 <u>Evaluate the severity of the Personal Data Breach</u>

5.2.1 Once a Personal Data Breach has been reported to the DPO, an initial assessment will be carried out by the DPO in conjunction with the Principal to establish the severity of the incident.

5.2.2 The DPO and the Principal will evaluate the severity of the Personal Data Breach by considering the following factors:

(a) the impact to the individuals concerned

- this is the overriding consideration in deciding whether a Personal Data Breach should be reported to the ICO.
- impact includes emotional distress as well as both physical and financial damage. It can include:
    - exposure to identity theft through the release of non-public identifiers, e.g. passport number
    - information about the private aspects of a person's life becoming known to others, e.g. health or medical conditions.

(b) the sensitivity of the Personal Data

- there should be a presumption to report to the ICO where smaller amounts of Personal Data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.
- this is most likely to be the case where the Personal Data Breach involves Special Category Personal Data. If the information is particularly sensitive, even a single record could trigger a report.

(c) the volume of Personal Data involved

- there should be a presumption to report to the ICO where:
  - a large volume of personal data is concerned, and
  - there is a real risk of individuals suffering some harm.
- it will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual.

(d) the number of individuals concerned.

(e) the potential media interest.

(f) the impact on the School.

5.2.3 Specific consideration will be given to whether Data Subjects will suffer any discrimination, identity fraud, financial loss, reputational damage, loss of confidentiality and economic or social disadvantage, as a result of the Personal Data Breach.

5.3 Containment and Recovery

5.3.1 The Principal, supported by the DPO, will take appropriate steps as necessary to contain the Personal Data Breach and recover the Personal Data as quickly as possible. Such steps will include (but are not limited to):

(a) immediately contain the Personal Data Breach (if this has not already occurred). Corrective action may include retrieval or recovery of the Personal Data, ceasing unauthorised access, shutting down or isolating the affected system;

(b) where the Personal Data Breach relates to a centrally managed ICT system, notify senior ICT/C2k staff immediately (as required);

(c) contact relevant staff to advise of precautionary measures where a risk remains live (as required);

(d) utilise expertise of staff within the School, Education Authority and external contractors as appropriate;

(e) attempt to retrieve misdirected emails and contact recipients to instruct them to delete and destroy the material sent to them in error;

(f) ensure that any codes or passwords are changed where the information has been compromised and that users are notified;

(g) assess the availability of back-ups where Personal Data is damaged/lost/stolen;

(h) whether there are wider consequences to the Personal Data Breach.

5.4 Notifications/Communications

Notification to Information Commissioner's Office

5.4.1 The DPO and the Principal will establish whether the Personal Data Breach needs to be reported to the ICO. Where the decision is taken to notify the ICO, the DPO will report the Personal Data Breach **within 72 hours** of the Personal Data Breach being initially discovered.

5.4.2 A decision to report or not to report the Personal Data Breach will be based on an assessment of the severity of the Personal Data Breach and any potential risk to the rights and freedoms of the Data Subjects.

5.4.3 Where a Personal Data Breach is reported to the ICO, the following information **must be** included within the report:

(a) a description of the of the Personal Data Breach;

(b) the categories and approximate number of individuals concerned;

(c) the categories and approximate number of Personal Data records concerned;

(d) the name and contact details of the DPO and where more information can be obtained;

(e) description of the likely consequences of the Personal Data breach; and

(f) a description of the measures taken, or proposed to be taken, to deal with the Personal Data Breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

5.4.4 ICO contact details are available at https://ico.org.uk/for-organisations/report-a-breach/.

Notification to Data Subjects

5.4.5 The Principal and the DPO will consider the need to notify the Data Subjects. This decision will be based on the risk to the rights and freedoms of Data Subjects. The Principal will notify the affected Data Subject(s) without undue delay, including:

(a) full details of the Personal Data Breach including a description of the Personal Data affected;

(b) the likely consequences of the Personal Data Breach;

(c) the measures we have or intend to take to address the Personal Data Breach, including, where appropriate, recommendations for mitigating potential adverse effects; and

(d) a name and contact point within the School.

5.4.6 When determining whether and how to notify Data Subjects of the Personal Data Breach, the School will:

(a) co-operate closely with the ICO and other relevant authorities, e.g. the police; and

(b) take account of the factors set out in **Appendix 2**.

Notification to the Police

5.4.7 The School will consider the need to contact the police for the purpose of containment and recovery. In addition, where it transpires that the Personal Data Breach arose from a criminal act perpetrated against the School, the School will notify the police and/or relevant law enforcement authorities.

Notifying Other Parties

5.4.8 The School, supported by the DPO, will consider whether there are any legal or contractual requirements to notify any other parties.

5.5 Evaluation and Response

5.5.1 Once the incident is contained, the Principal will lead a full review of:

(a) the cause(s) of the Personal Data Breach;

(b) the effectiveness of the response(s); and

(c) whether any changes to the systems, policies and procedures should be undertaken.

5.5.2 All staff, workers, contractors or volunteers employed or otherwise engaged at the School will be required to comply in full and promptly with any investigation.

5.5.3 An audit will be led by the Principal within 6 months from the date of report to ensure that recommendations have been implemented.

APPENDIX 1

Data Breach Report Form	
Time and Date Personal Data Breach was identified (Also time and date breach occurred if different to when identified)	
Who is reporting the breach: Name/Post/Dept	
Contact details: Telephone/Email	
Description of the Personal Data Breach:	
Volume of Personal Data involved and number of individuals affected	
Is the breach confirmed/suspected/ possible/threatened?	
Is the breach contained or ongoing?	
What actions are being taken to stop the breach and/or recover the data?	
Who has been informed of the breach?	
Any other relevant information	

Email form to dpo@eani.org.uk AND phone 028 8241 1300 to advise that a Data Breach Report Form has been sent.

Received by:	
Date/Time:	

APPENDIX 2

FACTORS AFFECTING IF AND HOW TO NOTIFY DATA SUBJECTS OF A PERSONAL DATA BREACH

Factor	Impact on obligation to notify data subject
Whether we have implemented and applied (to the affected personal data) appropriate technical and organisational protection measures—in particular measures that render the personal data unintelligible to any person who is not authorised to access it, e.g. encryption.	Where such measures have been implemented, it is not necessary to notify the data subject(s).
Whether we have taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data subjects affected by that breach is no longer likely to materialise.	Where such measures have been implemented, it is not necessary to notify the data subject(s).
Whether it would involve disproportionate effort to notify the data subject(s).	If so, it is not necessary to notify the data subject(s)—but we must, instead, issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
Whether there are any legal or contractual requirements to notify the data subject?	If yes, it may be necessary to notify the data subject(s) in any event.

Approvals	
Signatures:	
Principal	_____
Chair of Governors	_____
Date of approval by Governors:	____ / ____ / _____
Date of next annual review:	____ / ____ / _____