TABLE OF CONTENTS

INTRODUCTION

1.1 St. Mary's Christian Brothers' Grammar School (the "**School**") collects, holds, processes and shares large amounts of personal data, a valuable asset that needs to be suitably protected. As a Data Controller, the School must ensure that any processing of personal information for which it is responsible complies with the Data Protection Act 2018 ("**DPA**") and the UK General Data Protection Regulation ("**UK GDPR**") (together referred to as "**Data Protection Legislation**").

1.2 This Data Breach Management Procedure (the "**Procedure**") applies to all personal data held and processed by the School and is intended to provide guidance for school staff members on how a Personal Data Breach should be handled. It is intended for internal school use only but it is expected that the School will share certain aspects of the Procedure to the School's third party organisations who process personal data on its behalf.

1.3 The Procedure places obligations on school staff to report actual or suspected personal data breaches and sets out the steps to be followed by the School and its third party suppliers for managing, recording and investigating actual or suspected breaches. Every care is to be taken to protect personal data and to avoid a personal data breach, however, in such circumstances, it is vital that immediate action is taken to contain and remedy the breach.

1.4 The School's Data Protection Officer ("**DPO**") is legally required to notify the Information Commissioner's Office ("**ICO**") of any personal data breach within **72 hours** of the School becoming aware that a personal data breach has occurred if the breach is likely to result in a risk of adversely affecting individuals' rights and freedoms.

SECTION A

GENERAL INFORMATION

1. **Scope**

1.1 This Procedure sets out the steps to be taken by the School upon the occurrence of a personal data breach either from within the School itself or by a third party with whom the School has shared personal data e.g. a data processor. The purpose of the Procedure is to ensure that any personal data breach is dealt with in a consistent and effective manner in accordance with best practice guidelines.

1.2 Each potential personal data breach is different but experience shows that there are many seemingly harmless sets of circumstances that may, if not dealt with speedily, escalate to the level of a major incident. Prevention is better than cure and no-one will be criticised for treating an incident as serious in the first instance even if events later prove it is not.

1.3 This Procedure should be followed by all staff. It is an internal document and the School will share only particular aspects of the Procedure with these third parties. For example, the Data Breach Report Form should be shared with all data processors.

1.4 It is the responsibility of the Principal to ensure all staff, contractors, agents, consultants, data processors and other third parties who have access to School personal data are aware of this Procedure and follow the School's directions in the event of a data breach incident.

1.5 Where the School engages third parties to provide services which involve processing personal data, the services contract you have entered into with that third party or (where no such services contract is in place) the Data Processing Agreement between the School and the Data Processor should set out the third party's obligations in respect of handling a personal data breach.

2. **Must we report everything?**

2.1 The significance of a Personal Data Breach is a matter of judgement. However, in principle, all personal data breaches which are likely to result in a risk of adversely affecting individuals' rights and freedoms must be reported by the School's DPO to the ICO within 72 hours of the School becoming aware of the breach. Each actual or suspected personal data breach should be analysed on their own merits. The Principal (or Investigating Officer appointed by the Principal / Board of Governors), working with and through the School's DPO, will ensure appropriate reports are made to the ICO. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the School must also inform those individuals without undue delay. Note that there is a requirement to record all personal data breaches, regardless of whether the School is required to notify the ICO.

2.2 **All personal data breaches must be reported to the Principal (or their deputy) and the School's DPO immediately.**

2.3 Failure to notify ICO of a personal data breach when required to do so can result in a significant fine up to €10 million euros (or 2% of global turnover). The fine can be combined with other enforcement action such as issuing reprimands, imposing a ban on processing personal data or ordering that operational activities are brought into line and in accordance with UK GDPR requirements.

3. Approach

3.1 Adopting a standardised, consistent approach to all reported incidents in compliance with the Data Protection Legislation, aims to ensure that:

- immediate action is taken to manage a personal data breach incident;
- incidents are handled by appropriately authorised and skilled personnel;
- incidents are recorded and documented;
- the impact of the incidents are understood and action is taken to prevent further damage;
- external bodies or Data Subjects (defined below) are informed as required;
- incidents are dealt with in a timely manner and normal operations restored;
- evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny; and
- incidents are reviewed to identify improvements in policies and procedures.

4. Terminology

4.1 The following terminology is used in this Procedure:

Term	Meaning
Data Controller	A data controller determines the purposes and means of processing Personal Data and may share Personal Data with another data controller and/or data processor/s. As a data controller, you are not relieved of your obligations where a data processor is involved.
Data Processor	A data processor is responsible for processing Personal Data on behalf of a Data Controller. Data Protection Legislation places specific legal obligations on data processors, for example, to maintain records of personal data and processing activities. A data processor will have legal liability if they are responsible for a Personal Data Breach.
Data Subject	The individual to whom Personal Data relates.
Information Users	All staff, students, visitors, contractors and data processors acting on behalf of the School.
Joint Data Controller	Any other organisations that decide jointly with the School why and how personal data is processed.
Personal Data	Information relating to an individual who can be identified (directly or indirectly) from that information.

Term	Meaning
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.

5. What is a Personal Data Breach?

5.1 A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data or any security incident that affects the confidentiality, integrity or availability of personal data would be regarded as a personal data breach ("**Personal Data Breach**"). It 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.

- **How could personal data be "destroyed"?**

Personal Data that has been erased or irretrievably lost so that it no longer exists would be considered destroyed, e.g. the information has been corrupted. Similarly, if personal data no longer exists in a form that is of any use to the data controller.

- **How can personal data be "damaged"?**

Personal information would be regarded as damaged if it has been altered from its original form, is corrupted or is no longer complete. For example, if information has been encrypted by ransomware.

- **How can personal data be "lost"?**

'*Loss*' should be interpreted as the data may still exist, but the controller has lost control or access to it or no longer has it in its possession.

- **How can Personal Data be processed in an unauthorised or unlawful manner?**

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 Data Protection Legislation.

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

- loss or theft of Personal Data or equipment on which Personal Data is stored (e.g. loss of laptop, USB pen, iPad/tablet device/mobile phone, hard copy file or paper record);
- alteration of Personal Data without permission or authorisation;
- unauthorised disclosure of Personal Data;
- sending Personal Data to the wrong recipient;

- attempts (failed or successful) to gain unauthorised access to information or IT systems;
- loss of availability of Personal Data (e.g. hacking attacks);
- 'blagging' offences where Personal Data is obtained by deceiving the organisation who holds it;
- human error;
- an identified vulnerability or weakness which may lead to a Personal Data Breach.

5.3 A Personal Data Breach can have a range of adverse effects on individuals, including emotional distress and physical and material damage. Some Personal Data Breaches will not lead to risks beyond possible inconvenience to those who need the information to carry out their job whereas others can have significant consequences.

For example:

- a laptop is irreparably damaged but its files were backed up and can be recovered.
- the theft of a school database, where the information may be used to commit identity fraud.

5.4 Each case should be considered on its own merits taking account of a range of factors including those set out in **Appendix 4**

5.5 The Data Protection Legislation makes it clear that if a security incident takes place, the organisation must quickly establish whether a Personal Data Breach has occurred and take steps to address it.

6. Who is responsible under this Procedure?

6.1 **Information Users** must immediately report any actual, suspected, threatened or potential Personal Data Breach to the Principal (or their deputy). They must assist with investigations as required, particularly if urgent action is required to prevent further damage.

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

6.3 **The Principal** must ensure that all Information Users 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 usually the interface with the School's DPO. The School must immediately report any actual, suspected, threatened or potential Personal Data Breach to the School's DPO and it will usually be the Principal that does this, and then works closely with the School's DPO in relation to the Personal Data Breach.

6.4 Whilst the Principal is primarily responsible for ensuring that the School complies with this Procedure, the Principal (or the Board of Governors) may appoint an **Investigating Officer** (usually a member of the School's senior leadership team, such as a senior member of staff or a governor) to work with the School's DPO in relation to the investigation, assessment and reporting of a Personal Data Breach. In some circumstances, the School's DPO may recommend to the School that an Investigating Officer should be appointed (e.g. where investigation by the Principal is not deemed appropriate due to a potential conflict of interest).

6.5 **Data Processors** who become aware of a Personal Data Breach must notify the School without undue delay. The processor does not need to first assess the likelihood of risk arising from the breach before notifying the School although it can be useful if a brief assessment is undertaken so that the School has information on which to base whether or not a notification will be required to the ICO.

6.6 Where the school is in a **Joint Data Controller** relationship or an **Independent Data Controller** data sharing relationship and a Personal Data Breach occurs, the arrangements for managing the incident will be taken forward as set out and agreed in the relevant Data Sharing Agreement ("**DSA**") or Data Sharing Memorandum of Understanding (as appropriate).

6.7 **The School's DPO** is responsible for supporting the School in managing a Personal Data Breach in accordance with this Procedure and will be the point of contact with the ICO. Our DPO is the Education Authority. The School's DPO can be contacted at Education Authority, 40 Academy Street, Belfast BT1 2NQ or by email at [dpo@eani.org.uk]

7. Reporting a Personal Data Breach

7.1 The process for the School to follow upon discovery of a Personal Data Breach is set out at **Section B and Appendix 1.** A notifiable Personal Data Breach must be reported to the ICO by the School's DPO without undue delay and **no later than 72 hours** after becoming aware of it. The School would be considered to be aware of a Personal Data Breach when it has a reasonable degree of certainty that a security breach has occurred that led to Personal Data being compromised.

For example:

- If one of the School's online services was hacked and Personal Data potentially accessed by an unauthorised third party, the 72 hour window would begin when the service provider notified the School of the incident.

7.2 Any contract with a *data processor* should require that party to comply with the School's data breach management procedures (please refer to steps 1a, 1b, 2g and 5 of the Procedure). Where the School is sharing personal data with another *data controller* then both the School and that third party have a statutory requirement under Article 33 UK GDPR to notify the ICO of a personal data breach therefore it is likely that the third party will follow its own data breach processes.

7.3 Any failure to notify the ICO of a Personal Data Breach can incur an **administrative fine** of 2% of global turnover or **€10 million**. If the ICO considered that any of the data protection principles had been infringed e.g. integrity or confidentiality either by the breach or failure to report it, then the fine can be up to 4% of global turnover or **€20 million**.

7.4 Any member of staff who discovers an actual, suspected, threatened or potential Personal Data Breach must report it immediately to the Principal (or their deputy) as the primary point of contact. The incident should be logged in the School's data breach register.

7.5 Once notified of a Personal Data Breach, the Principal should report it at once to the School's DPO at dpo@eani.org.uk using the Data Breach Report Form set out in **Appendix 2** (where possible) followed up immediately by a phone call to the School's DPO on 028 8241 1300.

7.6 Any actual, suspected, threatened or potential Personal Data Breach discovered outside of normal working hours must be reported by calling the Principal (or their deputy) on 028 9029 4000. In writing to St. Mary's Christian Brothers' Grammar School, 147a Glen Road, Belfast, BT11 8NR or by email: info@stmarys.belfast.ni.sch.uk.

7.7 The 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. **Step 3** of **Section B** gives a preliminary list of the information generally sought by the School's DPO in their assessment of the situation.

7.8 When a Personal Data Breach has been reported to the School's DPO, the incident will be logged on a central system to facilitate effective management of the breach and to aid reporting. This will also assist in demonstrating accountability to the ICO who may ask to see this register.

7.9 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 Procedure may result in the matter being considered under the School's disciplinary procedure.

SECTION B

DEALING WITH A PERSONAL DATA BREACH

There is no single method of response to a Personal Data Breach. Incidents must be dealt with on a case by case basis by the School's DPO and the Principal (and/or Investigating Officer). The following list of actions while not exhaustive should be followed in the event of a personal data breach.

1. Assessing the Severity of the Personal Data Breach
2. Containment and Recovery
3. Notification to the Information Commissioner's Office (ICO) (where appropriate)
4. Notification to Data Subjects (where appropriate)
5. Notification to the Police / other parties (where appropriate)
6. Evaluation and Response.

1. STEP 1: Assessing the Severity of the Personal Data Breach

1.1 Some data breaches will not lead to risks beyond possible inconvenience to those who need the information to carry out their job. Before deciding on what steps are necessary further to immediate containment, the School (supported by the School's DPO) must assess the risks which may be associated with the breach, in particular, any adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

1.2 The following points may also be helpful in making this assessment:

- What type of data is involved?
- How sensitive is it? Some information is sensitive because of its personal nature (health records) while other types are sensitive because of what might happen if it is misused (bank account details).
- If information has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the information? If it has been stolen, it could be used for purposes which are harmful to the individuals to whom it relates. If it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the information, what could it tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
- How many individuals are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but it is certainly an important factor in the overall risk assessment.
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and therefore, your actions in attempting to mitigate those risks.

- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

1.3 Once the Principal (and/or Investigating Officer) has obtained information regarding the cause and extent of the Personal Data Breach, the Principal (or Investigating Officer) must notify the School's DPO. Where the Personal Data Breach has emanated from one of its data processors, it is essential they pass sufficient information to the School as quickly as possible following discovery of an actual or potential breach. This should be done by the data processor completing the Data Breach Report Form which should be provided to the data processor upon entering into a contract with them. The School may provide the data processor with the Data Breach Report Form at other times during its contractual relationship with that party, but it is best to do so at the outset of any contract.

1.4 When assessing the risk to individuals as a result of a Personal Data Breach, the School should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of it re-occurring. An assessment should take into account the following criteria:

- The type of breach
- The nature, sensitivity and volume of personal data
- Ease of identification of individuals
- Severity of consequences for individuals
- Special characteristics of the individual
- Special characteristics of the data controller
- Number of affected individuals

1.5 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. Further information is set out in Appendix 4).

2. STEP 2: Containment and Recovery

2.1 The Principal (and/or Investigating Officer), supported by the School's DPO, will take appropriate steps as necessary to contain the Personal Data Breach and recover the Personal Data as quickly as possible. Such steps may include (but are not limited to):

(a) 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 information within an ICT system, the Principal (or Investigating Officer) will notify the relevant senior ICT system provider's

staff immediately;

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

(d) utilise expertise of staff within the School, the School's DPO 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) consider whether there are wider consequences to the Personal Data Breach. In some cases, contact with external stakeholders, suppliers, contractors, agents, consultants, data processors and other third party users of the schools data may be required.

2.2 Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This may involve input from specialists such as:

- School's IT Security responsible person;
- School's Physical Security responsible person;
- School's Communications Office, etc.

2.3 In some cases, contact with external stakeholders, suppliers, contractors, agents, consultants, data processors and other third party users of the school's data will also be required.

2.4 The following actions should be carried out by the Principal (and/or Investigating Officer)**:**

(a) Establish who needs to be made aware of the breach and inform them what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of work, finding a lost piece of equipment or item of post, or simply changing access codes or passwords.

(b) Establish whether anything can be done to recover any losses and limit any damage the breach will cause. As well as the physical recovery of equipment or papers, this could involve the use of back-up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.

3. STEP 3: Notification to Information Commissioner's Office

3.1 The School's DPO and the Principal (and/or Investigating Officer) will establish whether the Personal Data Breach needs to be reported to the ICO. Where the decision is taken to notify the ICO, the School's DPO will report the Personal Data Breach **within 72 hours** of the Personal Data Breach being initially discovered by the School.

3.2 A decision whether 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. The following points are generally considered by the School's DPO in making an assessment of whether to report a Personal Data Breach to the ICO:

(a) **Nature of the Personal Data:** there may 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.

- What type of data is involved?
- How sensitive is it? Some information is sensitive because of its personal nature (health records) while other types are sensitive because of what might happen if it is misused (bank account details).
- If information has been lost or stolen, are there any protections in place such as encryption?

(b) **The impact to the individuals concerned:** this is the overriding consideration in deciding whether a Personal Data Breach should be reported to the ICO. It can include exposure to identity theft through the release of non-public identifiers, e.g. passport number or information about the private aspects of a person's life becoming known to others, e.g. health or medical conditions.

- What has happened to the information? If it has been stolen, it could be used for purposes which are harmful to the individuals to whom it relates. If it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the information, what could it tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and therefore, your actions in attempting to mitigate those risks.
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

(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.

- How many individuals are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but it is certainly an important factor in the overall risk assessment.

More detailed consideration of the points noted above is set out Appendix 4.

3.3 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 School's 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.

3.4 When notifying the ICO, you might wish to inform them if the media are aware of the breach so they can manage any increase in enquiries from the public.

3.5 It will not always be possible to fully investigate a breach within 72 hours. Article 34(4) UK GDPR allows the School to provide the required information in phases as long as this is done without further undue delay.

For example:

- An intrusion on our network is detected and we become aware that files containing personal data have been accessed. However, we don't know how the attacker gained entry, to what extent the data was accessed or whether the attacker also copied the data from the system. We notify the ICO within 72 hours of becoming aware of the breach, explaining that we do not yet have all the relevant details but that we expect to have the results of our investigation within a few days. Once the investigation uncovers details about the incident, we give the ICO more information about the breach without delay.

3.6 The ICO contact details are available on the ICO website. Providing the ICO with the required information in phases may be appropriate where the School has experienced a Personal Data Breach which needs to be notified to ICO but the School is satisfied it has been dealt with appropriately and / or if the School is still investigating a breach and will be able to provide more details at a later date. Alternatively, a breach can be reported by the School's DPO telephoning the ICO. This may be a helpful approach, in some cases, as the ICO can advise as to whether or not a formal report of the incident is, in fact, necessary.

4. **STEP 4: Notification to Data Subjects**

4.1 The Principal (and/or Investigating Officer) and the School's 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 more serious the breach, the more likely it is that an individual will want to take steps to protect themselves from the effects of the breach. The Principal (or Investigating Officer) 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 where more information can be obtained.

4.2 Any notification to affected individuals should have a clear purpose, whether this is to enable individuals to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints. The notification may also have to be made appropriate for children or vulnerable adults.

4.3 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 3

4.4 Note that the ICO has the ability to compel the School to notify affected individuals if it considers the breach to be a high risk.

5. **STEP 5: Notification to the Police / Other Parties**

5.1 The School, supported by the School's DPO, will (where appropriate) consider the need to contact the police and / or other parties 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 may notify the police and/or relevant law enforcement authorities.

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

6. **STEP 6: Evaluation and Response**

6.1 Once the Personal Data Breach has been dealt with, the Principal (and/or Investigating Officer) working with the School's DPO (and any third party involved in the Personal Data Breach), should undertake an evaluation of how the breach occurred, the manner in which it was dealt with and how future breaches can be prevented. For example, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable. Similarly, if the School's response was hampered by a lack of a clear allocation of responsibility, or staff training, then it is important to ensure these are reviewed and updated in the light of experience.

6.2 All Information Users employed or otherwise engaged at the School will be required to comply in full and promptly with any investigation.

6.3 Lessons learned from the breach should be documented and circulated to staff for the purpose of preventing a similar incident. The following points will assist you:

(a) Ensure you know what personal data is held in your area of responsibility e.g. pastoral care team, and where and how it is stored. Dealing with a data security breach is much easier if you know what information is involved. The School's information asset register is a useful starting point.

(b) Establish where the biggest risks lie. For example, how much special category personal data are you responsible for? Is personal data stored across your area of responsibility or is it concentrated in one location?

(c) Risks will arise when sharing personal data with or disclosing to others. You should ensure not only that the transmission is secure but also that only the minimum amount of data necessary is shared or disclosed. By doing this, even if a breach occurs, the risks are reduced.

(d) Identify weak points in your existing security measures such as the use of portable storage devices or access to networks.

(e) Monitor staff awareness of security issues and look to fill any gaps with training or tailored advice. Address such issues as when staff last received awareness training. The School's DPO can assist with this.

(f) Consider whether you need to establish a group of technical and non-technical staff to discuss 'what if?' scenarios. This would highlight risks and weaknesses as well as giving staff at different levels the opportunity to suggest solutions.

(g) Consider what lessons have been learnt and circulate these to relevant staff. Any recommendations for improvements should be implemented as quickly as possible and recorded as evidence that all reasonable steps have been taken to prevent recurrence at that time.

6.4 All Personal Data Breaches (whether reported to ICO or not) should be recorded by the School in a register (see **Appendix 5** for an example). The School could use the Data Breach Report Form (**Appendix 2**) as an aide to preparing an entry in the register.

APPENDIX 1

PERSONAL DATA BREACH MANAGEMENT PROCEDURE

	ACTION	CONSIDERATION	GUIDANCE/DOCUMENT
STEP 1: Assessing the Severity of the Personal Data Breach			
a.	**Within the first 30 minutes:** (a) where the personal data breach is discovered by a third party service provider, the third party should conduct a brief assessment of the incident to gather sufficient information for notification to the School and then notify the Principal/Deputy (b) where the personal data breach is discovered by a school staff member, this individual should inform the Principal/Deputy of actual/ potential/suspected Personal Data Breach	• who should staff notify if Principal/Deputy are not available? • note that 72 hour time period will start from the point of communication to the School (where the breach is discovered by a third party) or upon discovery (where the breach is discovered by a school staff member) • ensure the individual does not share information regarding the occurrence of the incident to any third parties, including data subjects, ICO, etc	
b.	Individual completes Personal Data Breach Report Form	• as much information should be included on the form as possible • ensure all staff have received training on how to complete the form. • ensure all data processors or third parties with whom the School has shared information are familiar with the form	**Document:** Data Breach Report Form (Appendix 2)
c.	**Within the first hour:** Principal (and/or Investigating Officer) to assess the situation and gather as much additional or supplementary information as possible to determine the severity and potential impact of the incident	• consider whether it is a breach that might require a report to ICO, data subjects, etc • consider whether any other individuals may need to be involved in managing the situation e.g. IT manager, C2k Helpdesk	**Guidance:** Section B, paras 1.2, 1.4
d.	Principal (or Investigating Officer) must notify the School's DPO of the incident.	• Record the incident on the School's data breach register	**Document**: Sample Personal Data Breach

	ACTION	CONSIDERATION	GUIDANCE/DOCUMENT
			Register for Schools (Appendix 5) **Guidance**: Section B, para 6.4
STEP 2: Containment & Recovery			
e.	**Within the first day:** Principal (and/or Investigating Officer) and School's DPO to work together to identify (where possible) any means of recovering the personal data	• e.g. restore data from backups, ensuring systems are being monitored for use of the data that has been compromised, recall / purge misdirected email, contact unintended recipients to instruct them to delete / destroy / return information sent in error etc.	**Guidance**: Section B, para 2.1
f.	Principal (and/or Investigating Officer) to consider measures to be implemented in order to contain the extent of any the breach	• Does a misdirected email need to be recalled and / or purged? • Does the School need to contact unintended recipients to instruct them to delete / destroy / return the information sent to them in error? • does a piece of equipment need to be located (e.g. laptop, USB stick)? • Do passwords or access codes need to be changed? • Where relevant, liaise with third party service provider to identify appropriate measures	
STEP 3: Notification to the ICO			
g.	The School's DPO to assess whether a notification to ICO is required	• deadline of 72 hours from School first becoming aware of the breach	**Guidance:** Section B, para 3.2, Appendix 4
h.	School's DPO to consider whether there is sufficient information in order to make a complete report. If not, School's DPO to notify ICO that information will be provided in phases		

	ACTION	CONSIDERATION	GUIDANCE/DOCUMENT
i.	If it is determined that the breach is serious enough to warrant a notification to the ICO, a report should be made by the School's DPO	• notifications By School's DPO can be made by the ICO by way of phone call, email or using the ICO's online form	**Guidance:** Section B, para 3.6 Document: ICO Website
STEP 4: Notification to Data Subjects			
j.	School's DPO to consider if the data subject(s) affected by the breach need to be notified?	• School's DPO needs to consider extent of breach, risk to the individual	**Guidance**: Section B, paras 4.1, 4.3 and Appendix 3
k.	If notification is required / appropriate, School's DPO to consider the form it should take		**Guidance**: Section B, para 4.1
STEP 5: Notification to the Police / Other Parties			
l.	School's DPO and Principal (and/or Investigating Officer) consider whether any other parties should be notified of the breach	• If there is any suspected criminal activity, the School should make a report to the Police • Consider whether any notification is required to a regulatory or statutory body, e.g. Education Authority or Department of Education • Where a third party service provider is involved, liaise with them as required	
STEP 6: Evaluation and Response			
m	School's DPO and Principal (and/or Investigating Officer) to review the circumstances of the breach to identify any lessons that could be learned		**Guidance**: Section B, para 6.3
n.	Implement new and/or amended policies and procedures (where appropriate) to minimise risk	• Liaise with the School's DPO / Education Authority where amendment to the policies/procedures may benefit other schools	

APPENDIX 2

PERSONAL DATA BREACH REPORT FORM

Data Breach Report Form	
Time and Date breach was identified (Also time and date breach occurred if different to when identified)	
How did you discover the breach, include details of who identified the breach (including whether internal or external source)	
If it has been more than 72 hours since the data breach, please explain reason for delay in reporting	
Who is reporting the breach: Name/Post/Dep	
Contact details: Telephone/Email	
Description of the Data Breach:	
Volume of 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?	

What are the potential consequences of the data breach?	
Who else has been informed of the breach?	
Date of the last Data Protection training for staff involved in this data breach	
Any other relevant information (e.g. is the data involved in the breach subject to any Data Sharing Agreement with a third party)	

For third party service providers/school staff who discover incident, please email form to for the attention of the Principal / Vice Principal

info@stmarys.belfast.ni.sch.uk. For Principal (or Investigating Officer), please email form to EA DPO dpo@eani.org.uk and phone EA DPO 028 8241 1300] to advise that a Data Breach Report Form has been sent.

APPENDIX 3

FACTORS AFFECTING THE DECISION TO NOTIFY DATA SUBJECTS OF A PERSONAL DATA BREACH

Informing data subjects that there has been a Personal Data Breach can be an important element in the breach management strategy. However, informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints. Considering the following factors should assist in deciding whether to notify individuals affected or other parties:

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. with 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 notification will help the individual bearing in mind the potential effects of the breach. Could individuals act on the information provided to mitigate risks, for example by cancelling a bank card or changing a password?	If yes, the data subject(s) should be notified
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.

APPENDIX 4

ASSESSMENT OF RISKS- CHECKLIST & CONSIDERATIONS

1. Summarised Checklist

- What has been lost/stolen or is unaccounted for – device and data, electronic media or paper?
- When and where was it lost and by whom (staff, data processor, contractor, etc.)?
- Was the data encrypted?
- Was the device encrypted?
- What type of personal data is involved?
- How many records are involved?
- How sensitive is it (medical information, bank details, etc.)?
- How many data subjects are affected?
- Who are they (pupils, parents, staff, etc.)?
- What is the risk to data subjects?
- Should they be notified of the incident?
- Does this incident need to be reported to the ICO/police?
- Is there a potential for press interest?

2. Detailed Considerations

All Personal Data Breaches must be reported to the School's DPO and recorded in the School's data breach register (regardless of whether or not they are reportable to ICO or the affected individuals).

A Personal Data Breach must be reported to the ICO within 72 hours of the School becoming aware of the breach, If it is likely to result in a risk of adversely affecting individuals' rights and freedoms. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the School must also inform those individuals without undue delay.

When assessing the risk to individuals as a result of a breach, you should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of it occurring. An assessment should take into account the following criteria:

The type of breach

The type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of potential consequences for an individual to a breach where an individual's medical details have been lost and are no longer available.

The nature, sensitivity and volume of personal data

A key factor is the type and sensitivity of the personal data that has been compromised. Usually, the more sensitive the data, the higher the risk the harm will be to the people affected. However, consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of a name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to the birth parent, the consequences could be very severe of both the adoptive parent and child. Breaches involving health data, identity documents or financial data, such as credit card details, can all cause harm on their own but, if used together, they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data.

Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A list of customers accepting regular deliveries may not be particularly sensitive but the same data about customers who have requested that their deliveries be stopped because they are on holiday would be useful information to criminals. Similarly, a small amount of highly sensitive personal data can have a high impact on an individual and a large amount of details can reveal a greater range of information about an individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.

Ease of identification of individuals

An important factor to consider is how easy it will be for someone who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match the personal data to a particular individual but it could be possible under certain conditions. Identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach and public availability of related personal details. This may be more relevant for confidentiality and availability breaches.

Personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without a decryption key. Additionally, appropriately implemented pseudonymisation can also reduce the likelihood of individuals being identified in the event of a breach. However, pseudonymisation techniques alone cannot be regarded as making the data unintelligible.

Severity of consequences for individuals

Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.

Whether the School is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk. There may be a confidentiality breach whereby personal data is disclosed to a third party or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong recipient within an organisation or to a commonly used supplier organisation. The School may request the recipient to either return or securely destroy the data it has received. In such cases, because the School has an ongoing relationship with them, and they may be aware of School's procedures, history and other relevant details, the recipient may be considered trusted. In other word, the School may have a level of assurance with the recipient so that we can reasonably expect that party not to read or access the data sent in error, and to comply with our instruction to return or destroy it.

Even if the data has been accessed, the School could still possibly trust the recipient not to take any further action with it, to return the data promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the School carries out following the breach. The fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the ICO or the affected individuals. Again, this will need to be assessed on a case-by-case basis. Nevertheless, the breach should still be recorded on the School's data breach register and a data breach report, and data breach assessment record completed as part of the general duty to maintain records of breaches. The school should also keep other relevant records or reports relating to its investigation of the of data breach and actions taken in response to it.

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.

Special characteristics of the individual

A breach may affect personal data concerning children or other vulnerable individuals who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of a breach on them, for example they may be members of the security forces or work in a particularly sensitive area.

Special characteristics of the data controller

The nature and role of the organisation and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal data, meaning there is a greater threat to individuals if their personal data is breached, compared with a mailing list.

Number of affected individuals

A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected.

General points

When assessing the risks that are likely to result from a breach, you should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and, similarly, where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, it is best to err on the side of caution and notify the ICO.

APPENDIX 5

SAMPLE PERSONAL DATA BREACH REGISTER FOR SCHOOLS

[ST MARY'S CHRISTIAN BROTHERS' GRAMMAR SCHOOL]

Incident Number	Date of Incident	Reported by	Summary of facts (including numbers affected, type and volume of personal data)	Cause of Breach	Remedial Actions	Notification to individual?	Reported to ICO?	Additional Comments

APPROVALS	
Principal:	
Chair of the Board of Governors:	
Date of Approval by Governors:	
Date of next annual review:	