ST. BRIGID'S SCHOOL

INFORMATION SECURITY BREACH PROCEDURE

October 2020

1 Purpose

1.1 In order to operate efficiently, St. Brigid's School has to collect and use information about people with whom it works with and for. These may include:

a) Members of the public;

b) Current, past and prospective pupils;

c) Current, past and prospective employees;

d) Current, past and prospective governors;

e) Clients and customers; and

f) Suppliers.

1.2 Organisations which process personal, and other sensitive, data must take appropriate measures against unauthorised, or unlawful, processing and against accidental loss, destruction of or damage to personal data. Many organisations take the view that one of those measures might be the adoption of a procedure on dealing with an information security breach incident.

1.3 Some key terms that are used in this procedure are:

- **Information Assets** – our data, files and documents in any format (paper and electronic);
- **Information Security Breach** – an activity which causes or may cause the loss, damage or corruption of data (examples are given in paragraph 2.2); and
- **Personal Data** – data which identifies a living individual either by itself or when matched with other data that would allow a clear identification to be made. Examples include – name, address, age, health, ethnicity etc.

1.4 This procedure has been developed using good practice published the Information Commissioner's Office (ICO). It will ensure that St. Brigid's responds appropriately and consistently to any actual or suspected breaches of that security, which may jeopardise its information assets and systems. This means that:

- A record is made of all such breaches;
- The breach is investigated thoroughly;
- An assessment is undertaken on the on-going risk;
- The breach is contained;
- Appropriate actions are taken to address the problem;
- Reports are made to external bodies, as required;
- There is proper monitoring and oversight;
- Any trends are identified and acted upon; and
- Lessons are learned and our information security is improved.

1.5 This procedure encompasses the above requirements and aims to:

- Reduce the impact of information security breaches by ensuring events and incidents are investigated and resolved appropriately;
- Identify areas for improvement to decrease the risk and impact of future breaches; and
- Protect the confidentiality, integrity and availability of our information assets at all times.

1.6 This document should be read in conjunction with the school's other information system policies and procedures – all of which are published on the school's website:

- Data Protection Policy
- Clean Desk / Clear Screen Policy and Procedure
- CCTV Policy
- Fair Processing Notice
- Complaints Policy

2 Context / Scope

2.1 This procedure applies to all St. Brigid's employees, governors, contractors and other third parties who may have information to our information assets.

2.2 The following are some examples of events that should be recorded using this procedure. The list is for guidance only and is not exhaustive; any event which potentially jeopardises the security of our information assets should be recorded, including:

- Theft, or loss, of any school IT equipment such as PCs, laptops, mobile phones etc.;
- Theft, or loss, of any other portable media storage such as; memory sticks, DVDs, CDs or other devices (whether encrypted or not);
- Any school computer infected by virus or other malware;
- Unauthorised access to databases containing personal and/or confidential information;
- Finding that data has been accessed and/or changed by an unauthorised party;
- Theft, loss or compromise of credit card data;
- Theft or loss of hard copy files containing personal and/or confidential data (including credit card data);
- Break-ins or other unauthorised access to buildings where personal data could have been viewed;

- Disclosures of data verbally, in writing or electronically to someone who should not have access to it;
- Not storing confidential information correctly so that it could be by unauthorised people;
- Accessing and/or making use of information for personal gain;
- Disposal of confidential information in a non-secure way; and
- Unauthorised personnel in restricted areas.

2.3 The consequences of an information breach can be severe. From an organisational perspective, an information security breach can result in financial penalties (up to £500,000), reputational damage, service disruption or even failure. Information security breaches may cause real harm and distress to the individuals they affect – lives may even be put at risk.

2.4 Disciplinary action could be issued against an employee that has found to have been negligent.

3 Procedure

3.1 Any event, which is likely to jeopardise the security of our information assets should be reported immediately using this procedure.

Step 1 – If a breach is suspected, the first step is to inform the Headteacher (or, in the absence of the Headteacher, the Business & Finance Manager).

Step 2 – The Headteacher (or Business & Finance Manager) must then contact the Chair Of Governors and DCC's ICT Service Desk (01824 706299) to report the breach. Depending on the nature of the breach, the Headteacher may also need to contact the following:

- Police, e.g. if there has been a theft or break in; and
- Caretaker, e.g. to make premises secure after any break in.

Step 3 – DCC's ICT Support Desk will record the breach within the 'Supportworks' system and then refer it onto DCC's Principal IT Security Officer for investigation (or, in the absence of the Principal IT Security Officer, DCC's Corporate Information Manager).

Step 4 – The Principal IT Security Officer will contact the Headteacher and arrange to meet within two working days to discuss the incident in greater detail.

Step 5 – The Principal IT Security Officer and Headteacher will meet, discuss the incident and complete an 'Information Security Incident Report Form' (see appendix 1). The purpose of the form is to create a record of the incident, which will include:

- Details of the breach;

- Identify the data affected*;
- Identify the likely impact of the breach;
- Assess the on-going risk;
- Identify the causes of the breach;
- Identify containment and recovery options;
- Identify who to notify;
- Agree upon a resolution or workaround; and
- Agree corrective actions to be taken to prevent reoccurrence, with target dates for their completion.

***** where information security breach involves the loss or compromise of personal data, the Principal IT Security Officer will consider notifying relevant parties such as the ICO, media and the individuals whose data has been lost or compromised.

Step 6 – The Headteacher will arrange the implementation of the agreed actions.

Step 7 - The Principal IT Security Officer will brief the Corporate Information Manager on the incident. Depending on the severity and likely impact of the incident, the Corporate Information Manager may choose to inform DCC's Head of Business Planning & Performance (and/or the Council's Senior Leadership Team) of the incident.

Step 8 – After a mutually agreed period of time after the event (maximum of 14 days), the Principal IT Security Officer and Headteacher will meet and review the progress of implementing the agreed corrective actions.

Step 9 – As progress is made, the Principal IT Security Officer will update the call on the Supportworks system and only close it down once (s)he is happy that the agreed actions have been effectively implemented.

Step 10 – The incident will be discussed at DCC's Information Governance Group. Any lessons learned will then be discussed with the aim of reducing the risk of it happening again.

Step 11 – The Principal IT Security Officer will review issues, trends and lessons learned arising from all incidents on a quarterly basis. Based on this review, (s)he will recommend any new measures to improve security. Recommendations could involve the development of; new policies, guidance, processes, communications and training as required.

4 Roles and Responsibilities

4.1 All school employees, governors, contractors and other third parties, who have access to our information assets, are responsible for:

- Ensuring the safety and security of that information and the systems that support it; and
- Following this procedure for reporting all information security breach incidents.

4.2 Headteacher

- To inform DCC's ICT Service Desk of an information security breach;
- To meet with DCC's Principal IT Security Officer, discuss the incident and assist with the completion of an 'Information Security Incident Form,;
- Agree the actions with the Principal IT Security Officer; and
- Arrange the implementation of the actions within the agreed timescales.

4.2 DCC ICT Service Desk

- Recording of all information security breach incidents on the 'Supportworks' system; and
- Referring all information security breach incidents onto Principal IT Security Officer for investigation.

4.3 Principal IT Security Officer

- Maintains overall responsibility for ensuring compliance with this procedure;
- Arranging to meet with the Headteacher;
- Completing an 'Information Security Incident Form';
- Coordinating and managing the response to any reported incident;
- Reporting regularly to the Corporate Information Manager on all security incidents;
- Analysing trends in information security breaches and recommending solutions;
- Managing the implementation of any recommended solutions;
- Reporting of incidents to external bodies, such as the ICO, if required; and
- Informing individuals affected, if required.

4.4 Corporate Information Manager

- Providing reports on information security breach incidents to the Head of Business Planning & Performance and Council's Senior Leadership Team; and
- Provide cover for DCC's Security and Standards Officer, if (s)he is unavailable.

5 DCC Quality Control and Monitoring Compliance

5.1 This procedure is jointly owned by the Principal IT Security Officer and Corporate Information Manager

6 Further Guidance

6.1 Further advice and guidance on this matter is available from the Principal IT Security Officer (01824 706229).

Appendix 1 - Security Breach Incident Form

Denbighshire County Council Information Security Breach Incident Form	
Date of Incident:	**Time of Incident:**
Date Reported:	**Time Reported:**
Name of person who discovered incident:	**Location of Incident:**
Reported by:	**Any other parties who have been involved** (Police, Caretaker etc.):
Department:	**Team:**
Description of the incident:	
Description of any IT equipment involved:	
Description of any information / data compromised:	
Media of information / data (paper, electronic, tape etc.):	
Cause of the breach:	
Assessment of impact and on-going risks:	
Recommended containment actions with agreed timescales:	
What steps have been or will be taken to recover records / data?	
(If applicable)	
What lessons have been learned from the incident and how will recurrence be prevented?:	
Date of follow-up meeting:	
Comments from follow-up meeting with progress of actions:	