ST. BRIGID'S SCHOOL

INFORMATION SECURITY BREACH PROCEDURE

October 2018

DENBIGHSHIRE SCHOOLS INFORMATION SECURITY BREACH REPORTING PROCEDURE

1 Purpose

1.1 In order to operate, all Denbighshire Schools have to collect and use information about people. This will include pupils, parents, current, past and prospective employees, and suppliers.

1.2 Schools shall process personal data taking 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, misuse or corruption of data; and
- **Security Incident Management** – this refers to the process by which an information security breach may be investigated and the related management procedures; 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, ethnic background etc.

1.4 This procedure has been developed based upon good practice published by the Information Commissioner's Office (ICO) and the Cabinet Office who are responsible for information assurance in the UK. Currently, Data Protection is not an area that has been devolved to the Welsh Government. This procedure will ensure that the School responds appropriately and consistently to any actual or suspected breaches of security, which may jeopardise its information assets and systems and will ensure compliance with government standards for reporting and handling incidents relating to information breaches. This means that:

- a record is made of all such breaches;
- the breach is investigated thoroughly with associated documentation produced;
- an assessment is undertaken on the on-going risk;
- the breach is contained;

- appropriate actions are taken to address the problem;
- management procedures exist to ensure and incident is handled correctly
- reports are made to external bodies and individuals 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.

2 Context/Scope

2.1.1 This procedure applies to all employees, supply staff, contractors and other third parties who may have access to our information assets.

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

2.1.3 Disciplinary action could be issued against any employee that has found to have been negligent.

2.1.4 The following are (non- exhaustive) examples of events that should be reported using this procedure. In summary, any event which potentially jeopardises the security of our information assets should be reported. It is also important that near-misses are reported to enable lessons to be learned and further protective measures to be considered.

- The theft or loss of any School IT equipment containing personal information such as laptops, mobile phones, USB stick, CD/DVDs;
- Theft or loss of any files or papers containing personal or confidential data;

- Break-in or other unauthorised access to a School building where personal data or official-sensitive information is stored and may have been put at risk; and
- Disclosures of personal data or official-sensitive information verbally, in writing or electronically to someone who should not have access to it.

3 Procedure

3.1 There are a number of steps involved in this procedure which are detailed below:

3.1.1 **Step 1** - If a breach is suspected, the first step is to ascertain if there are any steps you can take to immediately recover the information that might have been lost or stolen and inform your Line Manager immediately. Your Line Manager must then contact the Headteacher to report the breach. Depending on the nature of the incident, the Head (or a deputy in their absence) may also need to contact the following:

- Police, e.g. if there has been a theft or break in; and
- Facilities Management Staff to make premises secure after a break in;
- County Council's ICT service and the Corporate Information Unit where the breach has happened via a corporate or council hosted system.
- Consideration should be given as to what steps you can do in the short term in order to immediately retrieve the information.
- Where personal data has been lost or stolen or disclosed to unauthorised third parties then the Headteacher should inform the Schools' Data Protection Officer.
- Inform the data subject and the Chair of the Governing Body (where this is appropriate).

3.1.2 **Step 2** – The Data Protection Officer will record initial basic information regarding the incident within their central register.

3.1.3 **Step 3** – The Data Protection Officer will consider whether the issues are sufficiently serious or such that an investigation into how the breach has happened, who should be informed and advised on any further containment plan. They will contact the person reporting the incident in order to gather information about the reported incident in more detail. In certain circumstances, this may require a face-to-face meeting and staff must be made available to attend this meeting.

3.1.4 **Step 4** - The Data Protection Officer will, in consultation with relevant school staff, 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 circumstances 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.
- use the details on the form in order to consider whether to consult with the Council's Senior Information Risk Officer and the Corporate Information Unit as necessary and appropriate.

3.1.5 **Step 5** – Dependent upon the outcome of the investigation there might be a number of actions agreed at this stage. It will be the responsibility of the Headteacher to arrange for the implementation of the agreed actions.

3.1.6 **Step 6** - After a mutually agreed period of time after the event (maximum of 14 days), the Data Protection Officer will review the progress of implementing the agreed corrective actions.

4 Roles and Responsibilities

4.1 All employees, contractors, and other third parties who have access to the Schools' information assets are responsible for:

- ensuring the safety and security of that information and the systems that support it.
- following this procedure for reporting all information security breach incidents.
- co-operating and assisting with the completion of an 'Information Security Incident Form'.

4.2 Headteachers are responsible for:

- ensuring that a breach is reported appropriately by their staff;
- assisting with the completion of an 'Information Security Incident Form';
- arranging the implementation of the actions within the agreed timescales; and

- considering whether management action against the employee should be taken.
- Keeping the Governing Body informed as appropriate.
- Keeping the Head of Education and key County Council Education Officers informed as appropriate.

4.3 School's Data Protection Officer is responsible for:

- involved with investigating any incidents that involve the loss of personal data;
- act as the Data Protection Officer on behalf of the School;
- determine whether the incident is sufficiently serious it requires reporting to the ICO;
- if the ICO need to be informed to do so within 72 hours of the breach occurring;
- make any reports as necessary and act as the point of contact with the ICO in relation to the loss of personal data; and
- provide legal advice and assistance as required.

5 Quality Control and Monitoring Compliance

The School is the named Data Controller on the public ICO register and responsible in law. This procedure is owned by the School and it's Governing Body.

Appendix 1 – Security Breach Incident Form

Denbighshire Schools' Information Security Breach Incident Form	
Date of Incident:	**Time of Incident:**
Time Reported:	**Date Reported:**
Name of person who discovered incident:	**Location of Incident:**
Reported By:	**Any other parties who have been involved** (Police, Caretakers, ICT etc.):
Service:	**Department**
Detailed description of the incident:	
Details of any IT equipment or applications involved:	
Description of any information/data compromised:	
Media of information/data (paper, electronic file, USB, CD/DVD etc.):	
Any personal data involved?:	
Cause of the breach:	
Is there any on-going risk?:	**Y/N**
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:	

For Information Management use only: Include in this space any other relevant information in order to make any follow up recommendations or actions.		
Actions Agreed:		
Action 1:	**Deadline:**	
Action 2:	**Deadline:**	
Action 3:	**Deadline:**	
Follow-up Date:	**Officer Responsible for follow up:**	

Recorded on Central Register :	**Y/N**
Does this incident need reporting to the ICO?:	**Y/N**
Do the subjects need informing of the loss?	**Y/N**
Who will inform the data subject? (insert name of officer)	
How will the data subject be informed? (insert agreed method of communication)	
Have the individuals involved undertaken any DP training within last 12 months?	**Y/N**