Great Torrington School

Security Incident Management Procedure

1 Introduction

1.1 This procedure supports the School's Security Incident Management Policy and applies to staff, agents, Governors, contractors and partners of Great Torrington School. The intention of this procedure is to ensure that an information security incident is reported, monitored and handled appropriately. It is intended that this procedure will help ensure that the School is able to respond to an information security incident appropriately and in a way that lessens the impact on a data subject. This policy is also in place to help the School to ensure appropriate learning from incidents takes place, and to ensure that reoccurrences do not happen in future.

2 Scope

2.1 This procedure applies to the reporting, investigation and management of an information security incident as defined by section 2 of the Security Incident Management Policy.

3 Procedure review

2.1 This procedure will be reviewed by the Data Protection Officer on an annual basis. Formal requests for changes should be sent to the Data Protection Officer:

Jon Buss, dpo@gts.devon.sch.uk, 01805 623531

4 Reporting a security incident

4.1 Members of the public and members of staff should report an information security incident to the Data Protection Officer as soon as possible. "Near misses" must also be reported as it is important that the School is aware of any risks that might expose our information to future incidents.

4.2 Those wishing to report an information security incident can remain anonymous if they prefer and are therefore not required to provide their name or contact details when reporting an incident. However, this information may be useful when identifying and investigating the information security incident. The information provided during notification of an incident will be treated sensitively and securely, although it may be necessary to share information provided during notification of an incident, with senior leaders and for serious incidents, to the Human Resources Department.

5 Logging a security incident

5.1 The Data Protection Officer is responsible for overseeing information security incident investigations. Upon being notified of an information security incident the Data Protection Officer will undertake the following actions:

- Log the incident on the School's Data Breach Log within 2 working days of receipt.
- Acknowledge receipt of an information security incident notification within 2 working days of receipt.
- Gather sufficient information to enable a risk assessment or Privacy Impact Assessment to be undertaken within two working days of receipt.
- Carry out an assessment of the severity of the incident within 3 working days of receipt.
- Notify the Information Commissioner's Office or relevant supervisory authority within 72 hours of becoming aware of an information security incident that might adversely affect the rights and freedoms of a data subject.

5.2 Every information security incident will be categorised according to the nature of the incident, the sensitivity of the information involved and where relevant, the number of data subjects affected. If it is not possible to categorise the incident at the point of notification (due to insufficient information provided) this will be established during the incident investigation.

5.3 If when logging an information security incident, it becomes apparent that a particular team or service is repeatedly causing the same type of security incident, or, if an individual member of staff is the cause of regular security incidents, the Human Resources Department will be advised, and they in accordance with the person's line manager will consider whether or not disciplinary action should be taken.

6 Incident classification

6.1 Great Torrington School will classify every information security incident according to the following criteria.

Incident classification	Description
No incident	The actions which gave rise to the incident notification have not jeopardised the confidentiality, availability or integrity of the School's information.
No incident – near miss	There is a risk that the actions which gave rise to the incident notification, might adversely affect the confidentiality, availability or integrity of the School's information. However, this risk has not materialised in this case.
Low risk incident	The confidentiality, availability or integrity of the School's information has been adversely affected. However, the impact of this incident on the School is negligible. If the incident involved personal data, the incident has not impacted adversely on the rights and freedoms of the data subject.
Medium risk incident	The confidentiality, availability or integrity of the School's information has been significantly affected such that there is a measurable impact on the School. If the incident involved personal data, the incident has not impacted adversely on the rights and freedoms of the data subject.
High risk incident	The confidentiality, availability or integrity of the School's information has been significantly impacted to such an extent that there are significant business continuity risks, reputational risks or risk of regulatory action. If the incident involved personal data, the incident has caused a negative effect on the rights and freedoms of the data subject.

7 Incident notification to key staff

7.1 The Data Protection Officer must be notified in the event of an information security incident within the following timeframes, according to the perceived level of risk. Other relevant staff may also be notified as appropriate.

- High risk incidents will be notified within 1 working day.
- Medium risk incidents will be notified within 2 working days.
- Low risk incidents will be notified within 5 working days.
- No incident and near misses will be notified as soon as possible.

8 Security incident notification to the Information Commissioner's Office

8.1 In accordance with Article 33 of the GDPR, the School is committed to notifying the Information Commissioner's Office or relevant supervisory authority within 72 hours, of being notified of information security incident that might adversely affect the rights and freedoms of a data subject.

8.2 Notifications are the responsibility of the Data Protection Officer, who will ensure that the risks associated with information security incidents are recorded, monitored and where appropriate escalated in accordance with the School's Information Assurance Policy. Such incidents will be

handled as a high risk incident and will be subject to the notification arrangements outlined in Section 7 of this procedure.

9 Information security incident investigation

9.1 The Data Protection Officer will notify the all key staff in accordance with Section 7 of this procedure. They will then complete an information security incident investigation and notify the relevant key staff with the outcome within 20 working days of the School being notified of the incident.

9.2 The notification and investigation report will include a summary of the incident, lessons to be learned, action points for the team involved to implement, good practice recommendations and links to any relevant guidance.

9.3 Where an information security incident involves the inappropriate disclosure of personal data, action will be taken immediately by investigating officer or the relevant service, to retrieve the data in question.

9.4 If during an information security incident investigation, it has become apparent that the actions of the staff member who caused an incident, were negligent, malicious or were unreasonable in the circumstances, the investigating officer will consult the Human Resources Department who will decide if a conduct investigation is necessary. Staff found to have acted in a negligent or malicious manner will be disciplined in accordance with the School's Disciplinary Policy.

9.5 Where the actions of a staff member are found to constitute an offence under data protection legislation and or the Computer Misuse Act 1990, the matter will be reported by the Data Protection Officer to Devon and Cornwall Police Constabulary.

10 Notifying data subjects

10.1 All information security incidents that are likely to negatively impact on the rights or freedoms of a data subject, will be notified to the ICO / Data Subject by the School without undue delay. Such notifications will include the following information:

- An apology for the incident which has occurred.
- A description of the information put at risk.
- A description of any risk that this incident might cause the data subject.
- A description of how the incident occurred.
- Details of any steps taken by the School to remedy the incident and prevent a reoccurrence.
- Guidance on how the data subject can protect themselves from the effects of the information security incident.
- Details of how the data subject can make a formal complaint to the School and the Information Commissioner's Office.
- Details of who the School has notified about the incident in question.

10.2 All notifications under Section 10 of this procedure will be made verbally over the telephone, in person or in written form.

11 Review of information security incidents

11.1 The Data Protection Officer will ensure that the information risks associated with information security incidents are recorded, monitored and escalated to senior leadership in accordance with the School's Information Assurance Policy.

11.2 Actions proposed in response to an information security incident investigation will be monitored by the Data Protection Officer and will be reported to Information Asset Owners every quarter. Trends in information security incidents will also be monitored, with corrective action proposed to services on a quarterly basis.

11.3 Any corrective action which has not been undertaken in response to information security incident investigation will be escalated to key staff as identified in Section 7 of this procedure. Decisions taken in respect of corrective action will be informed by a risk assessment or Privacy Impact Assessment.

11.4 If improvements identified in an information security incident investigation have not been made by particular staff members, and / or if similar security incidents have been reported involving the actions of a particular staff member, the Data Protection Officer will notify the line manager of the staff member concerned. The senior leadership of the department in question will also be alerted along with the Human Resources Department, who will decide if disciplinary action is necessary. High risk incidents will also be notified to the Head Teacher.

12 Information security incident record keeping

12.1 The officer responsible for carrying out an information security incident investigation will ensure that robust records are kept of their investigation. Where possible, the investigation will be informed by discussions with key personnel including interviews with the staff member(s) responsible for the incident. Records will be retained for the duration of the security incident investigation and in accordance with the School's Data Retention Policy.