OWLS Academy Trust

Security Breach Management Plan & Policy

Last updated: 25 April 2017

Contents:

Statement of intent

1. Legal framework
2. Enacting the security breach management plan
3. Containment and recovery
4. Assessment of risks
5. Consideration of further notification
6. Evaluation and response
7. Monitoring and review

Appendices

a) Timeline of Incident Management

Statement of intent

The OWLS Trust is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the school are only accessible by the appropriate individuals. It is therefore important to uphold high standards of security and precaution, and to have systems and procedures in place that support this – such as the **E-Security Policy**.

The school recognises, however, that breaches in security can occur, particularly as the majority of information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, it is necessary to have a contingency plan, and procedures in place to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

For the purposes of this policy, the title of '**data controller**' will be used in reference to the person(s) primarily responsible for the handling of information and data within a school.

Signed by:

Headteacher Date:

Chair of governors Date:

1. Legal framework

1.1. This policy has due regard to statutory legislation and regulations, including, but not limited to, the following:

- The Data Protection Act 1998
- The Computer Misuse Act 1990
- The General Data Protection Regulation (GDPR), coming into effect as of 25 May 2018

1.2. This policy has due regard to the school's policies and procedures including, but not limited to, the following:

- **E-Security Policy**
- **E-Safety Policy**
- **Data Protection Policy**

2. Enacting the security breach management plan

2.1. Data security breaches require more than just an immediate response to identify and contain the situation; they also require longer-term recovery planning. This will pull together the views and expertise of various individuals and groups from across the school – input may be necessary from IT, HR and legal departments, and in some cases from external authorities, stakeholders and suppliers.

2.2. These processes start once the breach has been detected, with the initial procedure being run in the following four-step process – containment and recovery, assessment of risks, consideration of further notification, and evaluation and response.

3. Containment and recovery

3.1. The school's **data controller /IT lead at each school**, **and headteacher**, will take the lead in investigating the breach, and will be allocated the appropriate time and resources to conduct this.

3.2. The **data controller**, as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or compromised.

3.3. The **data controller** will oversee a full investigation and produce a comprehensive report.

3.4. The cause of the breach, and whether or not it has been contained, will be identified – ensuring that the possibility of further loss/jeopardising of data is eliminated or restricted as much as possible.

3.5. Any further action which could be taken to recover lost or damaged data will be identified. This includes the physical recovery of data, as well as the use of back-ups.

3.6. The school will establish what steps need to be taken to prevent further data loss which will require support from various school departments and staff. This action will include:

- Informing relevant staff of their roles and responsibilities in areas of the containment process.
- Taking systems offline.
- Retrieving any lost, stolen or otherwise unaccounted for data.
- Restricting access to systems entirely or to a small group.
- Backing up all existing data and storing it in a safe location
- Reviewing basic security, including:
  - Changing passwords and login details on electronic equipment.
  - Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

3.7. Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the **data controller** will inform the police of the security breach.

4. Assessment of risks

4.1. The following questions will be considered by the **data controller** in order to fully and effectively assess the risks that the security breach has brought, and to help take the next appropriate steps. All relevant questions should be clearly and fully answered in the **data controller**'s report and records:

- What type and how much data is involved?
- How sensitive is the data? Sensitive data is defined in the Data Protection Act 1998; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details).
- Is it possible to identify what has happened to the data – has it been lost/stolen/deleted/tampered with?
- If the data has been lost/stolen, were there any protective measures in place to prevent this, such as data and device encryption?

- If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of back-up tapes and spare copies?

- Has individuals' personal data been compromised – how many individuals are affected?

- Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?

- Could their information be misused or manipulated in any way?

- Could harm come to individuals? This could include risks to the following:

  - Physical safety

  - Emotional wellbeing

  - Reputation

  - Finances

  - Identity

  - Private affairs

- Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence/damage to the school's reputation, or risk to the school's operations?

- Who could help or advise the school on the breach? Could the LA, external partners, authorities, or others provide effective support?

4.2. In the event that the **data controller,** or other persons involved in assessing the risks to the school, are not confident in the risk assessment, they will seek advice from the Information Commissioner's Office (ICO).

5. Consideration of further notification

5.1. The school will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in security (see 5.8 onwards for specific GDPR requirements about personal data).

5.2. The school will decide whether notification will help the school meet its security obligations under the seventh data protection principle.

5.3. The school will assess whether notification could help the individual(s) affected, and whether individuals could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password.

5.4. If a large number of people are affected, or there are very serious consequences, the ICO will be informed.

5.5. The school will consider whom to notify, what to tell them and how they will communicate the message, which may include:

- A description of how and when the breach occurred and what data was involved. Details of what has already been done to respond to the risks posed by the breach will be included.
- Specific and clear advice on the steps they can take to protect themselves, and what the school is willing to do to help them.
- A way in which they can contact the school for further information or to ask questions about what has occurred.

5.6. The school will consult the ICO for guidance on when and how to notify them about breaches.

5.7. The school will consider, as necessary, the need to notify any third parties – police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies – who can assist in helping or mitigating the impact on individuals.

Under the GDPR, the following steps will be taken if a breach of personal data occurs:

5.8. The school will notify the ICO within 72 hours of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

5.9. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the school will notify those concerned directly with the breach.

5.10. Where the breach compromises personal information, the notification will contain:

- The nature of the personal data breach including, where possible:
  - The type(s), e.g. staff, pupils or governors, and approximate number of individuals concerned.
  - The type(s) and approximate number of personal data records concerned.
- The name and contact details of the **data controller** or other person(s) responsible for handling the school’s information.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed, to deal with and contain the breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

6. Evaluation and response

6.1. The **data controller** will establish the root of the breach, and where any present or future risks lie.

6.2. The **data controller** will consider the data and contexts involved.

6.3. The **data controller** and **headteacher** will identify any weak points in existing security measures and procedures.

6.4. The **data controller** and **headteacher** will identify any weak points in levels of security awareness and training.

6.5. The **data controller** will report on findings and, with approval of school leadership, implement the recommendations of the report after analysis and discussion.

7. Monitoring and review

7.1. This policy will be reviewed by the **headteacher**, in conjunction with the **data controller**, on an **annual** basis.

7.2. The **data controller** is responsible for monitoring the effectiveness of this policy, amending necessary procedures and communicating any changes to staff members.

Timeline of Incident Management

Date	Time	Activity	Decision	Name/position	Date