Procedures for Reporting and Handling Data Breaches

2023 - 2024

Version	2
Document authors	Sam Proctor
Other contributors	IGS
Procedures produced (date)	December 2023
Procedures to be reviewed (date)	December 2024
Other related policies	Data Protection Policy Data Handling Security Policy Data Breach Policy Complaints Policy Procedures for Reporting and Handling Security Incidents Policy Whistle-blowing Policy

Roles within the school

Data Protection Officer (DPO) - Ms. L. Almond

Senior Information Risk Owner (SIRO) - Mr. S. Proctor

Information Champion (IC) - Mrs. J. Pitcher

Information Governance Governor - Mrs. S. Stronach

School Data Protection Role Contact Details

Role	Name	Email contact
Data Protection Officer (DPO)	Ms. L. Almond	IGS@essex.gov.uk
Senior Information Risk Owner (SIRO)	Mr. S. Proctor	admin@westthurrockacademy.co.uk
Information Champion (IC)	Mrs. J. Pitcher	admin@westthurrockacademy.co.uk
Information Governance Governor	Mrs. S. Stronach	Chair@westthurrockacademy.co.uk

Introduction

This document applies to everyone who undertakes duties on our behalf (including third parties, suppliers, partners and contractors etc.). We have a duty to ensure that the information we process, and hold, is secure. We will react appropriately to any actual or suspected data breaches relating to information, systems and data.

We recognise there are risks associated with individuals accessing and handling information in order to conduct our business and have in place Policy and Procedures which need to be followed. Data breaches occur when those policies are not followed. Therefore there is a need to report these breaches to manage the risks and identify improvements to decrease the number of future breaches.

Where an external supplier has reported a data breach it is the responsibility of the school to report the breach to the ICO where it meets the threshold to do so.

Quick Reference Guide to activities for managing data breaches

- Report the breach to the school office;
- Use the Outcome Report template to gather basic information about:
    - i. what has happened
    - ii. who is involved
    - iii. what has been done to manage the breach already
- From this information, classify the data breach using the criteria at Appendix A;
- If the risk scoring works out at 3 or more, then escalate to the SIRO providing the Outcome report ;
- Ensure the SIRO and DPO are involved in investigating major/critical and escalated breaches and collect evidence as required;
- Seek advice on ‘moderate’ breaches from the DPO;
- Ensure remedial action is taken within 24 hours to recover unlawful disclosure of personal/ sensitive information;
- Provide advice, support and intervention as appropriate to each case;
- Inform data subjects (parents/ guardians, employees) where appropriate and always where there is a risk of harm;
- Identify and manage consequent risks of the breach;

- Identify expected outcomes, stakeholders and any policies or standards that may have been breached;
- Complete the Breach Outcome Report and update your B1 reporting template;
- Following receipt of Outcome Reports analyse results looking at lessons learnt and implement required actions;
- Preserve evidence and maintain an audit trail of events and evidence supporting decisions taken in response to the breach;
- Retain records of all breaches as evidence of the how the process works;
- Develop and implement an appropriate means of preventing similar breaches in the future.

Policy References

This procedure is a requirement of the Data Breach Policy.

Procedures

What is a Data Breach?

An data breach is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of information and weaken or impair business operations.

An information security event indicates that the security of an information system, service, or network may have been breached or compromised. An information security event indicates that an information security policy may have been violated or a safeguard may have failed.

See ‘Appendix B: Breach Types’ for a comprehensive list of what is considered a breach. There are some examples below:

- Using, or being asked to use, another person’s login or password (or both);
- Not locking your PC/ laptop before leaving it, if you are logged in;
- Allowing confidential information to be passed on to people who do not have the correct authorisation to see it or not preventing this;

- Sending personal information to the wrong recipient, either by email or post;
- Stolen or lost electronic equipment, including laptops or mobile phones;
- Sending abusive emails, or forwarding racist or sexist jokes or emails;
- Allowing someone to enter the building without an appropriate security check, e.g. signing in process;
- Intentional or accidental infection of computer viruses or unauthorised software.

Employee Responsibilities

Anyone discovering a data breach, even those they think are minor, must immediately report it to the school office.

No retaliatory action will be taken against any member of staff who reports a data breach about another member of staff in good faith, regardless of the seriousness of the data breach or the level of individual responsible for the breach. Identification of a reporting party who requests anonymity shall be protected to the degree feasible but cannot be guaranteed.

Investigations

The Headteacher or school information champion will classify the data breach using the scoring system at Appendix A, and an investigator will be assigned. The Headteacher, as SIRO, will oversee all major breaches to ensure they can assess and recommend a report to the Data Protection Officer (DPO) for the matter to be considered for notification to the ICO if required. The school office should seek advice from the DPO for breaches they consider ‘Moderate’.

Timescales

The assigned breach investigator will contact those involved within 4 working hours of being notified of the breach and will agree initial actions to be taken. Depending on the complexity of the breaches the timescales for completing investigations will vary. Data breach Classifications can be found in Appendix A.

However, listed below are the expected timescales for the majority of breaches to be investigated and closed:

Minor/Near Miss (Scale = 1) – closure within 1 week

Medium (Scale = 2) – corrective action within 24 hours, investigation of cause of breach, implement preventative action and outcome report within 2 weeks

Major/Critical (Scale = 3) – corrective action within 24 hours; investigation of cause to begin immediately and implement preventative action, including recommendations to Governors/Trust and outcome report to be completed within 1 month. Notification of major breaches requiring assessment for ICO notification must be sent to the DPO within 24 hours of becoming aware of the breach.

Reporting to the ICO

The Information Commissioner requires major breaches of Data Protection law to be reported within a statutory timescale. Your DPO will assess the need for notification according to the threshold dictated by the ICO.

It is the Senior Information Risk Owner's (SIRO) responsibility to decide whether to report a breach to the regulator; the Information Commissioner's Office (ICO) after consultation with the DPO.

The ICO state that they require notification of breaches where the breach "is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage". Each case must be assessed on a case-by-case basis and should involve the opinion of the DPO.

If the breach is considered to represent a ‘high risk’ to the data subject rights (i.e. it is a higher level of risk still than that requiring reporting to the ICO), then there is a further requirement that the data subjects themselves are formally notified by the School. The opinion of the DPO should be taken into account by the SIRO.

If the ICO is to be notified about the breach, the notification must contain:

- The nature of the breach including the categories and approximate number of the:
    i. individuals concerned
    ii. personal data records concerned
- The name and contact details of the DPO or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach;
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach;
- The measures taken to mitigate any possible adverse effects.

A notifiable breach has to be reported to the ICO under the GDPR within 72 hours of the School becoming aware of it. The law recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases; however the initial notification – if it is necessary to notify - must happen within the timescale.

If the breach is sufficiently serious to warrant notification to the public, the School must do so without delay.

The reasons behind the SIRO’s decision whether or not to notify must be documented on the Data Breach Outcome Report Form and must include consideration of the DPO’s opinion.

Advice and Support

If you have any issues over the clarity of these procedures, how they should be applied in practice, require advice about exemptions from the requirements or have any suggestions for amendments, please contact your SIRO.

Breach Statement

A breach of this procedure is a breach of the Data Breach Policy. Breaches will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendix A: Risk Classification

Any incident scoring 3 would be reportable to the SIRO and DPO for consideration of further reporting to the ICO, if it scores less, it is not. If in doubt please refer to SIRO for a decision.

1. **As defined by Data Protection Law, is the data:**

- Special Category (Sensitive) (1)
- Personal (0)

2. **Has the law been breached?**

- Yes (1)
- No (0)

3. **Did the data get sent:**

- Within the school (0)
- To an external partner organisation, e.g. NHS/ Social Care (1)
- To an external organisation/ individual (2)

4. **Has the school applied the appropriate technical security (e.g. is the information encrypted, appropriate access controls in place, correct procedure followed):**

- Yes (0)
- No (1)

Appendix B: Breach Types

The following is a list of data breach examples which fall within the scope of the Policy and this Procedure. This is not an exhaustive list.

Breach Categories & Types:

3rd Party/Supplier

- Receiving information from third parties not intended for our school;
- Our suppliers lose information from our school, or sends information of our school to an incorrect recipient.

Breaches of Policy

- Leaving a computer screen (laptop or desktop) unlocked when unattended;
- Spam emails, abusive messages, improper use of mailing lists;
- Accessing sites in business time, inappropriate sites, use of un-authorised online systems;
- Misuse of position, access, or identity for personal gain;
- Adding an unauthorised personal device to the network or storing schools' information on a personal device;
- General lack of good information handling;
- Password for system does not match agreed standard creating additional risk.

Mis-sent emails

- Sending an email to the wrong person;
- Auto-complete not checked when sending an email, and the wrong recipient selected.

Lost/ Stolen Equipment

- Lost equipment;
- Theft of equipment.

Network/cyber Security

- Spam emails received that pose a threat to the Network;
- Critical System offline;
- Threat of virus to the network;
- Reset or corruption of folder permissions for folders on the network;
- Network accessed by individuals with no lawful right of access;
- Ransomware attack;
- Member of staff has shared password of a system with another member of staff;
- Member of staff has logged someone into a system under their own username without sharing the password.

Data Sharing

- Information shared with another person/organisation without ensuring they had a legal right to the information.

Physical Security

- Unauthorised person has been able to access a building or secured area;
- Building or storage facility discovered to be insecure;
- Member of staff has lost building pass.

Mis-sent letters/files

- Letter sent to the wrong person/wrong address;
- Letter has been sent to estranged mother/father of child including other parent’s contact details without permission;
- School file sent to the wrong school.

Published in error

- Photo published on social media when consent had not been given.

BCC in email not used

- Email sent to parents of whole class including their email addresses in the CC instead of the BCC.

Misuse of information

- Member of staff using parent email addresses for personal matter (e.g. to inform them of setting up a business outside of the school) without permission;
- Member of staff reviews a parent record for personal reasons or personal gain, not connected with the school.

Info sent insecurely

- Email containing sensitive personal information sent without using secure email or password protection;
- Letter containing sensitive personal information sent without using secure delivery method.