Data Breach Policy

2023 - 2025

Version	1 - Supersedes all previous versions (Formally known as Security Incident Policy)
Document authors	Mr. S. Proctor
Other contributors	IGS
Policy produced (date)	October 2022
Policy to be reviewed (date)	October 2024
Other related policies	Data Protection Policy Data Handling Security Policy Acceptable Personal Use Policy Statutory Request Policy Privacy Notice Complaints Policy Whistleblowing 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

What is a Security incident?

A data breach is a confirmed breach, potential breach or 'near-miss' breach of one of the school's information policies.

What I must do	Why I must do it	How I will do it
If you discover a security incident, you must immediately report it.	Capturing data breaches allows us to respond effectively when something has gone wrong. Capturing all types of data breaches allows us to understand where our weaknesses are, how well our policies are working and what we should change about our policies to make them more effective.	Please notify the school office. No action will be taken against any member of staff who reports a data breach about another member of staff in good faith. Identification of a reporting party who requests anonymity shall be protected as far as is feasible.
When reporting the incident, you must provide as much information as possible.	To help us quickly assess the severity of the breach and to speed up the investigation.	Include full details of the breach such as dates, names and any remedial action that has been taken.
The Investigating Officer must complete investigations and complete an outcome report (see Procedures for Reporting or Handling a Data Breach).	Carry out an effective process appropriate to the severity of the breach.	Where appropriate, undertake the following: A. Identify expected outcomes, stakeholders and any policies breached. B. Speak to staff involved. C. Record evidence and keep an audit trail of events and evidence supporting decisions taken. D. Get expert help. E. Escalate. F. Inform data subjects (service users, staff) where appropriate. G. Identify and manage risks of the breach.

		H. Commence disciplinary action, or record why not. I. Develop and implement a communications plan where appropriate. J. Put in place controls to prevent recurrence. K. Complete the Breach Outcome Report.
All staff must support investigations into breaches as required.	Carry out an effective process appropriate to the severity of the breach.	Where appropriate, undertake the following: A. Work with the SIRO to investigate major data breaches. B. Assess the outcome to ensure the appropriate action has been taken. C. Provide knowledge and advice, and carry out any recommended actions for major or critical breaches, where required.
Maintain a full record of each breach from reporting to closure.	Ensure the process is followed to completion.	Undertake the following: A. Classify the data breach. B. Verify the details and oversee the investigation. C. Work with SIRO to investigate major data breach. D. Advise, support and intervene as appropriate. E. Review Breach Outcome Reports and close.

The Headteacher/SIRO must support the investigation of major and critical breaches.	Ensure that there is appropriate resource, expertise and independent scrutiny of processes for higher impact breaches.	For major and critical incidents: A. Undertake the investigation (critical only). B. Work with DPO (major only). C. Assess if it is necessary for the security incident to be reported to the ICO. D. Complete an outcome report and recommend remedial actions.
Comply with the timescales and escalation process outlined in our Procedures for Reporting or Handling a Data Breach.	Ensure that all breaches are handled in a timely manner.	Follow the process outlined in the school's Procedures for Reporting or Handling a Data Breach.
Major and critical breaches must be referred to the Data Protection Officer.	Ensure that serious breaches are reviewed against the criteria for reporting to the regulator.	Use contact details the school hold for the DPO. This contact can also be made via IGS.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting Mr. S. Proctor (Head Teacher - SIRO - admin@westthurrockacademy.co.uk)

Breach Statement

Breaches of Information Policies 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.

Contacts

If you have any enquires in relation to this policy, please contact Mr. S. Proctor (the school's Head Teacher) on 01708 866 743 or admin@westthurrockacademy.co.uk . The Head Teacher will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office - www.ico.gov.uk

References

- Data Protection Act 2018
- UK GDPR