Security Incidents Policy

First approved by Trust Board: July 2018
Review Frequency: Annually

Date of last review: September 2020
Date of next review: September 2021

Version Control

Author/Reviewer	Date Created	Version	Notes
IGS	July 2018	1.0	
IGS/K. Draper	July 2019	2.0	Roles pre-populated for ease of use Additional point 8 added Other minor updates for ease of use
K. Draper	September 2020	2.1	No amendments

Openness   Honesty   Social Responsibility   Caring for Others

Osborne Co-operative Academy Trust

Osborne Co-operative Academy Trust is a multi-academy trust (MAT) incorporated around the principles and values of the international co-operative movement. These are Equality, Equity, Democracy, Self-help, Self-Responsibility and Solidarity, along with the ethical values of openness, honesty, social responsibility and caring for others. These values and principles underpin all our actions.

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

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. *MUST*: If you discover a security incident, you must immediately **report** it
2. *MUST*: When reporting the incident, you must **provide** as much information as possible
3. *MUST*: The Investigating Officer must **complete** investigations and complete an outcome report (see Procedures for Reporting or Handling a Security Incident)
4. *MUST*: All staff must support investigations into incidents as required
5. *MUST*: Maintain a full **record** of each incident from reporting to closure
6. *MUST*: The Headteacher/SIRO must support the investigation of **major and critical** incidents
7. *MUST*: Comply with the timescales and escalation process outlined in our Procedures for Reporting or Handling a Security Incident
8. *MUST:* Major and critical incidents must be referred to the Data Protection Officer.

Why must I do it?

1. Capturing security incidents allows us to respond effectively when something has gone wrong. Capturing all types of security incidents 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
2. To help us quickly assess the severity of the incident and to speed up the investigation
3. Carry out an effective process appropriate to the severity of the incident
4. Carry out an effective process appropriate to the severity of the incident
5. Ensure the process is followed to completion
6. Ensure that there is appropriate resource, expertise and independent scrutiny of processes for higher impact incidents
7. Ensure that all incidents are handled in a timely manner
8. Ensure that serious incidents are reviewed against the criteria for reporting to the regulator.

How must I do it?

1. Report immediately to the CEO or Headteacher, (or their Deputy if they are unavailable) or if you would like to stay anonymous kate.draper@osborne.coop. No action will be taken against any member of staff who reports a security incident about another member of staff in good faith. Identification of a reporting party who requests anonymity shall be protected as far as is feasible.
2. Include full details of the incident such as dates, names and any remedial action that has been taken.
3. 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

3

      g. Identify and manage risks of the incident
      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 Incident Outcome Report

4. Where appropriate, undertake the following:
   a. Work with the SIRO to investigate major security incidents.
   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 incidents, where required.

5. Undertake the following:
   a. Classify the Security Incident
   b. Verify the details and oversee the investigation
   c. Work with Central Trust and School Leads to investigate major security incidents.
   d. Advise, support and intervene as appropriate
   e. Review Incident Outcome Reports and close

6. For major and critical incidents:
   a. Undertake the investigation (critical only)
   b. Work with Central Trust and School Leads (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.

7. Follow the process outlined in the school's Procedures for Reporting or Handling a Security Incident

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 Kate Draper, Trust Secretary, email kate.draper@osborne.coop

If you believe the policy does not meet your business needs, you may raise this with your Information Champion who, if they agree with your suggestion, may propose a policy change.

Document Control

Version:	2.1
Date approved:	September 2020
Approved by:	Osborne Co-operative Academy Trust Board
Next review:	September 2021 (annual review)

References

- Data Protection Act 2018

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.

Openness   Honesty   Social Responsibility   Caring for Others