Security Incidents Policy

A security incident is a confirmed breach, potential breach or 'near-miss' breach of one of ECC'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 Information Champion must **complete** investigations as directed by the Senior Information Risk Owner and complete an outcome report (see Procedures for Reporting or Handling a Security Incident) maintaining a full **record** from reporting to closure.
4. ***MUST***: Data Protection Officer must support the investigation of **major and critical** incidents
5. ***MUST***: Comply with the timescales and escalation process outlined in our Procedures for Reporting or Handling a Security Incident [with link]

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, ensure the process is followed to completion.
4. Ensure that there is appropriate resource, expertise and independent scrutiny of processes for higher impact incidents
5. Ensure that all incidents are handled in a timely manner.

How must I do it?

1. Report the incident immediately, even if out of hours, to the Headteacher either in person, by telephone on 01245 472686 or by email to admin@galleywood.essex.sch.uk. 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. Classify the security incident.
    e. Inform data subjects (service users, staff) where appropriate
    f. Identify and manage risks of the incident
    g. Commence disciplinary action, or record why not
    h. Develop and implement a communications plan where appropriate
    i. Put in place controls to prevent recurrence
    j. Complete the Incident Outcome Report
    k. Work with the Data Protection Officer to investigate major security incidents.
    l. Review Incident Outcome Reports and close
4. For major and critical incidents:
    a. Undertake the investigation (critical only)
    b. Work Senior Information Risk Owner (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.
5. Follow the process outlined in the ECC 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 our Data Protection Officer – Lauri Almond at Lauri.Almond@essex.gov.uk or call 0333 0130975.

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:	1
Date approved:	23rd May 2018
Approved by:	Sarah Manning
Next review:	[May 2019 + Annually]

References

- Data Protection Act 1998
- Article 8, Human Rights Act 1998

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.