Chelmsford County High School For Girls

Data Breach Policy

Deleted: Security Incidents

Last Amended: Oct 2018	Committee Responsible for Review: Management	
Last Approved: Sep 2022	Date of Next Review: Sep 2024	Model: Essex Information Governance Support C7

Data Breach Policy

A data breach 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 data breach, you must immediately **report** it to the Headteacher and Business Manager
2. ***MUST***: When reporting the incident, you must **provide** as much information as possible
3. ***MUST***: The Business Manager/ Line Manager must **complete** investigations as directed by the Headteacher and/or Data Protection Officer and complete an outcome report (see Data Breach Management Procedure: R:\Staff\Miscellaneous\Policies\3 - Procedures)
4. ***MUST***: The Business Manager must support investigations as directed by the Headteacher and/or Data Protection Officer and provide an **outcome report**
5. ***MUST***: The Headteacher must oversee and support each investigation, maintaining a full **record** from reporting to closure
6. ***MUST***: The Data Protection Officer must support the investigation of **major and critical** incidents
7. ***MUST***: Comply with the timescales and escalation process outlined in our Data Breach Management Procedure: R:\Staff\Miscellaneous\Policies\3 - Procedures

Why must I do it?

1. 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
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.

Deleted: Security Incidents

Deleted: security incident

Deleted: security incident

Deleted: Security Incident

Deleted: Security Incident

Deleted: security incidents

Deleted: security

Deleted: incidents

How must I do it?

1. Email or speak to the Headteacher and Business Manager. 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.
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
    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 Headteacher, Business Manager and Data Protection Officer to investigate major data breaches.
    b. Assess the outcome to ensure they are satisfied the appropriate action has been taken.
    c. Provide service area knowledge and advice, and to carry out any recommended actions within their function for major or critical incidents, where required.
5. Undertake the following:
    a. Classify the Data Breach
    b. Verify the details and oversee the investigation
    c. Work with relevant staff to investigate major data breaches.
    d. Advise, support and intervene as appropriate
    e. Review Incident Outcome Reports and close
6. For major and critical incidents:

Deleted: security

Deleted: incident

Deleted: security incidents

Deleted: Security Incident

Deleted: security incidents

a. Undertake the investigation (critical only)
b. Work with Data Protection Office and relevant staff (major only)
c. Assess if it is necessary for the data breach 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 Data Breach

Deleted: security incident

Deleted: 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 the Headteacher.

Deleted: . 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: 4

Date approved:

Approved by: Management Committee

Next review: Biennial – September 2025

Deleted: 3

Deleted: 23/09/2024

Deleted: 4

References

- Data Protection Act 1998
- UK GDPR

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.