St Benedict's Catholic College

Data Breach Policy

Date reviewed	August 2023
Approved by governors	September 2023
Version	2023
Date of next review	August 2024

Data breachs Policy

A data breach is a confirmed breach, potential breach or ‘near-miss’ breach of one of the college’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
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 Data breach)
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 Data breach
8. ***MUST:*** Major and critical incidents must be referred to the Data Protection Officer.

Why must I do it?

1. Capturing data breachs allows us to respond effectively when something has gone wrong. Capturing all types of data breachs 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. Please notify the college 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.
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 SIRO to investigate major data breachs.
    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 Data breach
    b. Verify the details and oversee the investigation
    c. Work with SIRO to investigate major data breachs.
    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 SIRO (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 ECC Procedures for Reporting or Handling a Data breach

What if I need to do something against this 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 business manager.

References

- Data Protection Act 2018 (including the UK General Data Protection Regulation)

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.