ROBERT CLACK SCHOOL

SECURITY AND DATA BREACH POLICY

If printed, copied or otherwise transferred from this website this document must be considered to be an uncontrolled copy.

Policy amendments may occur at any time. Please consult the Policies page on the website for the latest update.

Controlled Document

Title	Security Incident and Data Breach Policy
Author	Data Protection Enterprise Ltd
Owner	Headteacher
Document Version	Version 5
Created	August 2026
Approved by	Approved in accordance with the School's governance arrangements
Review Date	August 2029 or earlier where there is a change in the applicable law affecting this Policy Guidance

Version Control

Version	Date	Author	Description of Change
1	16/08/18	Data Protection Enterprise www.dataprotectionenterprise.co.uk	New Policy
2	01/08/2019	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	Annual Review Contents list added
3	20/01/2020	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	Policy Review S9 Added
4	23/08/2023	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	Policy Review Amendments to: Section 1
5	August 2026	Data Protection Enterprise Ltd www.dpenterprise.co.uk	Policy review. Updated for the Data (Use and Access) Act 2025, current ICO breach guidance, controller accountability and cyber incident reporting.

Contents:

1. INTRODUCTION

The School is aware of its responsibilities under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025 (DUAA 2025). It will use appropriate technical and organisational measures to protect the personal data it holds.

The DUAA 2025 amended aspects of UK data protection law and its relevant provisions are reflected in this policy.

Every care must be taken to protect information and prevent security incidents. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It may affect the confidentiality, integrity or availability of information. The School will respond promptly to all suspected incidents, contain any harm and follow its Breach Management Plan where personal data may be affected.

Compliance with UK data protection law is a legal requirement. Failure to manage a breach appropriately may expose individuals to harm and may result in regulatory action, reputational damage, operational disruption or financial loss.

The School takes cyber security seriously and follows recognised best practice, including guidance from the National Cyber Security Centre (NCSC) and the Department for Education's digital and technology standards. Staff must complete appropriate cyber security training, use multi-factor authentication where available, handle portable devices securely and report suspicious emails or incidents promptly.

All individuals permitted to access personal data in line with their work must agree to comply with this policy and agree to undertake any relevant training that may be appropriate.

2. PURPOSE

The purpose of this policy is to ensure a standardised management approach in the event of a serious security incident, including the handling of a data breach. Security incident management is the process of handling security incidents in a structured and controlled way ensuring they are dealt with:-

- speedily and efficiently
- consistently
- ensuring damage is kept to a minimum (i.e loss of equipment (laptop/memory stick) and/or loss of personal data)
- ensuring that the likelihood of recurrence is reduced by the implementation of appropriate measures.

3. SCOPE

This policy applies to all personal data processed by or on behalf of the School, in any format, including paper, electronic, audio and visual records. It applies to governors, staff, volunteers, contractors and others who have access to the School's information.

This policy takes effect immediately and all staff should be made aware of security incident requirements. Any queries should be directed to the Data Protection Officer (contact details below).

It includes personal data processed in third-party systems used by the School, such as cloud-based MIS and assessment platforms. Processors and other service providers must notify the School without undue delay if they become aware of a personal data breach affecting School data, in accordance with their contract and UK data protection law.

4. TYPES OF SECURITY INCIDENTS

This policy addresses the reporting and handling of security incidents and data breaches.

A data security breach can happen for many reasons:

- Loss or theft of information or equipment on which information is stored, such as laptops, mobile phones or encrypted removable media
- Unauthorised disclosure of personal information
- Inappropriate access controls allowing unauthorised use
- Breach of physical building access/security
- Human error e.g. personal information being left in an insecure location, using incorrect email or postal address, uploading personal information to a website
- Unforeseen circumstances such as fire or flood
- Cyber attack, malware or ransomware
- Social engineering, where information is obtained through deception or impersonation ("blagging")
- Misdirected emails or attachments containing personal or sensitive data
- Unauthorised verbal disclosure of personal information

5. REPORTING A SECURITY INCIDENT

This section explains how to report a security incident including a data breach.

- Anyone who discovers or suspects a security incident MUST report it immediately to the Data Protection Officer and, in any event, no later than 24 hours after discovery, using the security incident form at Appendix A. They must also take any safe and proportionate immediate steps requested to contain the incident but must not delete evidence. If the DPO is unavailable, a member of the senior leadership team must be informed. Incidents discovered outside normal working hours must be reported through the School's urgent reporting route as soon as possible; the 72-hour regulatory period runs from the point at which the School becomes aware of a personal data breach.

- The Data Protection Officer will coordinate the assessment and advise the School. The Headteacher, IT support, safeguarding lead and others may assist according to the nature and severity of the incident. Staff must not conduct their own investigation or contact affected individuals unless instructed to do so.

- The Headteacher, on behalf of the School as controller, retains responsibility for decisions about serious incidents and regulatory notification, taking advice from the Data Protection Officer.

- Any decision to take disciplinary action will be in line with the School's disciplinary policy.

- The security incident report will be concluded when all investigations are complete.

- All suspected security incidents will be logged for monitoring and audit purposes. The record will include the facts, effects, remedial action and, where a personal data breach is not reported to the ICO, the reasons for that decision.

6. BREACH MANAGEMENT RESPONSIBILITIES OF THE DATA PROTECTION OFFICER

Breach Management Plan

The Data Protection Officer will coordinate the response and advise the School, following the ICO's recommended breach-management approach:

i. Containment and Recovery
ii. Assessment of risk to individuals
iii. Notification, where required
iv. Evaluation and response

I. Containment and Recovery

Containment and recovery involves limiting the scope and impact of the data breach including, where necessary, damage limitation.

The Data Protection Officer will:

- Lead the investigation
- Identify who must be involved and what they must do to contain the incident, for example isolating a system, recalling an email, recovering equipment, changing credentials or preserving evidence.
- Establish what can be recovered and take steps to limit the harm the breach may cause.
- Where notification is required, ensure the ICO is informed without undue delay and, where feasible, within 72 hours of awareness; and
- Where appropriate, involve IT support and notify the police, Report Fraud, the NCSC, insurers, the Department for Education or another relevant body
- For a cyber incident, the School will activate its cyber response arrangements and seek urgent technical support. Regulatory, law-enforcement and cyber reports serve different purposes; making one report does not remove the need to consider the others.

ii. Assessing the risks

The Data Protection Officer will advise on the risk to individuals by considering the potential adverse consequences, their seriousness and the likelihood of them occurring. Children and vulnerable individuals may be at greater risk and this will be taken into account.

In making this assessment the Data Protection Officer will assess:

- What type of data is involved
- How sensitive it is
- If data has been lost or stolen are there any protections in place such as encryption
- What has happened to the data
- What are the consequences if a third party has the data
- How many individuals and records are affected, and who those individuals are
- What physical, material or non-material harm may result
- If there are wider consequences to consider such as a risk to public health or loss of public confidence

iii. Notification

The Headteacher will decide, taking advice from the Data Protection Officer, whether the ICO and affected individuals must be notified. Staff must not make notifications directly unless authorised. A notifiable breach must be reported to the ICO without undue delay and, where feasible, within 72 hours after the School became aware of it. If all information is not yet available, an initial report may be made and further information supplied in phases. Any delay must be explained.

The ICO must be notified where the personal data breach is likely to result in a risk to individuals' rights and freedoms. Where the breach is likely to result in a high risk, affected individuals must also be informed without undue delay unless a statutory exception applies. Communications will use clear language and explain the nature of the breach, likely consequences, action taken and a contact point. Each incident will be assessed on its own facts.

iv. Evaluation and response

The Data Protection Officer will:

- fully review both the causes of the breach and the effectiveness of the response to it
- maintain a breach log containing the information required by Article 33(5) UK GDPR
- report findings and recommendations to the Headteacher
- implement an action plan to correct identified issues if required
- monitor staff awareness of security issues and look to fill any gaps through training
- consider whether the breach reveals a need to update the School’s policies, supplier contracts (e.g. data processing agreements), or training programmes.

- Evaluate the School's compliance with the data minimisation and pseudonymisation principles, particularly for data transmitted externally.

7. DATA PROTECTION OFFICER DETAILS

Data Protection Enterprise Ltd
Mobile: 07511 290724
Email: info@dpenterprise.co.uk

8. POLICY REVIEW

The DPO is responsible for monitoring and reviewing this policy. Although this policy is reviewed every three years, changes to legislation, national guidance, codes of practice or advice from the Information Commissioner advice may trigger interim reviews. The DPO will highlight any significant legislative developments that may require earlier action or updates to this Policy.

The School will keep this policy under review in light of the DUAA 2025, ICO guidance and relevant education-sector cyber security standards.

9. LINKS WITH OTHER POLICIES

This Security Incident and Data Breach policy is linked to the School:

- Data Protection Policy
- Freedom of Information Policy
- CCTV Policy
- Data Protection Impact Assessment Policy
- Third-Party Data Sharing Protocols
- Acceptable Use Policy
- Information Security Policy
- Safeguarding Policy
- Privacy Notices

The Information Commissioner provides a free helpline and a wide range of guidance and resources relating to information rights and data protection. Further information is available from: Information Commissioner Office (ICO)

Appendix A

SECURITY INCIDENT AND DATA BREACH

NOTIFICATION FORM

Report immediately: Send this form to the Data Protection Officer at info@dpenterprise.co.uk as soon as a security incident is discovered or suspected. Do not wait until every detail is known. Do not contact affected individuals or delete evidence unless instructed.

1. Person reporting the incident

School	
Name and job title	
Telephone number	
Email address	

2. Incident overview

Date incident occurred		**Time**	
Date incident discovered		**Time**	
Who discovered it?		**Location / system**	

Brief description of what happened **State the facts known at this stage, including how the incident was discovered.**

☐ Email or attachment sent to the wrong person	☐ Information disclosed verbally or by post
☐ Lost or stolen device / paper records	☐ Unauthorised access or inappropriate permissions
☐ Phishing, malware, hacking or ransomware	☐ Information altered, deleted or unavailable
☐ Information published or uploaded in error	☐ Other (describe above)

3. Personal data involved

☐ Names and contact details	☐ Pupil or staff identifiers
☐ Education, attendance or assessment records	☐ Employment or payroll information
☐ Special category data	☐ Safeguarding information
☐ Criminal offence information	☐ Financial or account information
☐ Passwords or access credentials	☐ Photographs, audio or video

Describe the personal data involved **Include the level of detail, sensitivity and whether the information was encrypted, password-protected or otherwise secured.**

Approximate number of individuals affected	
Approximate number of records affected	
Whose information is involved?	☐ Pupils ☐ Parents/carers ☐ Staff ☐ Others
Are any individuals particularly vulnerable?	☐ No ☐ Yes - give details below

Recipients or people who may have accessed the information. Give names or organisations where known. State whether they are trusted recipients and whether they have confirmed deletion or return.

4. Immediate containment

What action has already been taken? For example: recalled email, contacted trusted recipient, disabled account, changed password, isolated device, recovered records or contacted IT support.

Has the information been recovered, returned or securely deleted?	☐ Yes ☐ No ☐ Partly ☐ Not known
Has IT support been informed?	☐ Yes ☐ No ☐ Not applicable
Is the incident still ongoing?	☐ Yes ☐ No ☐ Not known
Preserve evidence: Do not delete emails, logs, messages or other evidence. Follow instructions from the DPO, senior leadership and IT support.	

5. Potential effect on individuals

What harm could result? Consider distress, embarrassment, discrimination, safeguarding risk, identity theft, fraud, loss of confidentiality, reputational damage or loss of control over information.

Have any individuals complained or raised concerns?	☐ Yes ☐ No
Have affected individuals been contacted?	☐ No ☐ Yes - authorised by: _____
Supporting evidence attached	☐ Email / screenshot ☐ IT report ☐ Recipient confirmation ☐ Other

Submit now: Email the completed form and any supporting evidence securely to info@dpenterprise.co.uk Further information can be supplied later.