David Ross Education Trust

Broadening Horizons

Data Incident Response Policy

Document Management Information

Applicable to:	All staff in all Academies and Central Support Services including individuals employed by the Trust, contractors and agency staff. All Members and Trustees.
Dissemination:	The policy will be available to staff via the Trust's Policy Centre
Implementation:	Applicable to all DRET academies
Training:	Mandatory awareness training for all staff, with additional role-based training for Data Champions, IT staff and incident response leads.
Review Frequency:	The policy will be reviewed every three years. The policy will also be reviewed earlier if needed in the light of new evidence/legislation/guidance
Policy Author:	Head of Data Protection and Compliance, George Selby
Executive Policy Owner:	Director of Governance, Maria Maltby
Approval by:	Executive Team
Approval Date:	19 October 2026
Next Review Due:	October 2029

Revision History

Document version	Description of Revision	Date Approved
1.0	Version approved by Risk and Audit Committee	25 March 2021
1.1	Executive review in line with review frequency. Minor typographical changes made	2 July 2024
1.2	Minor update following audit. Clarification around non-compulsory use of Data Incident Response Form.	7 November 2024
1.3	Strengthening of wording. No material changes.	19 October 2026

Contents

Contents 3
1. Introduction 4
2. Policy Scope 4
3. Definitions 4
4. The Trust's Policy on Data Incident Response 4
5. Reporting and Consequences of Non-Compliance 13
6. Policy Status 13
7. Related Policies 13

1. Introduction

1.1. The David Ross Education Trust as the Data Controller is responsible for protecting the personal data that it collects, uses, stores and otherwise processes.

1.2. The Trust recognises that even after technical and organisational measures are implemented to protect personal data, vulnerabilities remain, accidents can occur and controls may fail.

1.3. In addition, previously unidentified threats may occur, for example a cyber-attack. This means incidents or serious personal data breaches are possible.

1.4. The purpose of this policy is to outline the procedures to be followed by Trust employees in the event of a suspected data breach. It is intended to enable the Trust and its academies to assess, contain and respond to incidents in a timely fashion and to help mitigate the potential harm to individual data subjects.

1.5. This Data Incident Response policy identifies and describes the role and responsibilities of nominated academy and Head Office staff in responding to a suspected data breach. It does, however, remain the overarching responsibility of all staff and employees to be absolutely scrupulous when it comes to the handling, storage and deletion of personal data; whether it's about us or about our students or parents/carers. Adopting this approach will help the Trust limit and prevent breaches of personal data in the first instance.

2. Policy Scope

2.1 This policy applies to staff within the Trust.

2.2 It is the responsibility of all individuals in the Trust to familiarise themselves with this policy and comply with its provisions.

2.3 The Data Incident Response policy applies to the loss of any data pertaining to a data subject whose data is owned or processed by the Trust, our academies or any third party processing data on the Trust's behalf.

3. Definitions

3.1 **Trust** means all Academies within the David Ross Education Trust, as well as Head Office and central services operations.

3.2 **Executive Leadership Team** means the Chief Executive Officer ("CEO") and the direct line management reports of the CEO (the "Directors").

4. The Trust's Policy on Data Incident Response

4.1 Personal Data Incidents

4.1.1 A personal data incident occurs when there is an event giving rise to the potential for accidental, unauthorised or unlawful access, acquisition, alteration, destruction, disclosure, loss or misuse of personal data. For example:

- Lost, stolen or misplaced documents or devices.
- Improper disposal, misdirected emails, accidental posting on public sites or malicious hacks.
- Unauthorised modifications to personal data, attacking its integrity.
- New, unauthorised, use of personal data collected for a different purpose.

4.1.2 The examples above illustrate that events ranging from a lost laptop or mobile phone, to cyber-attacks impacting vast amounts of personal data are all relevant. Until the suspected breach has been properly investigated the Trust will not understand the potential risk to personal data.

Quick action: if you suspect a breach If you become aware of an actual or suspected personal data breach, you must: contain the issue if safe to do so; notify the Data Champion, DPO or dataprotection@dret.co.uk immediately; preserve evidence and do not delete suspicious emails, files or logs; record what happened and when; notify IT immediately where a cyber or device-related incident is suspected; and avoid delaying notification while full details are gathered.

4.2 Reporting Requirement

4.2.1 The David Ross Education Trust, as the Data Controller, is required to assess all suspected personal data breaches under UK GDPR and the Data Protection Act 2018. Where a breach is likely to result in a risk to individuals' rights and freedoms, the Trust must notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, within **72 hours** of becoming aware of the breach.

Trust IT must be engaged where the incident involves systems, devices, accounts, email, cloud services, networks, malware, cyber attack, credential compromise or suspected unauthorised access.

4.2.2 Academies and third parties processing personal data on behalf of the Trust must notify the Trust immediately and without undue delay when they become aware of an actual or suspected personal data breach. The Trust will be treated as aware once the relevant academy, processor, Data Champion, DPO or other appropriate Trust representative has enough information to reasonably conclude that a personal data breach may have occurred.

4.2.3 Failure to report an incident or suspected personal data breach can be as detrimental as the breach itself, as the Trust may be unable to contain the incident, mitigate risks, meet statutory reporting timescales or learn lessons from what happened.

4.2.4 The David Ross Education Trust as the Multi Academy Trust is the Data Controller and therefore determines the purposes for which personal data is processed (the 'why' and the 'how').

4.3 Incident Response Approach

4.3.1 Personal data breaches can occur at any time and the Trust requires an approach that enables incidents to be identified, contained, investigated, assessed and, where necessary, reported within the statutory **72-hour** timeframe under UK GDPR.

4.3.2 In order to meet this timeline there needs to be an approach which covers all eventualities, including an incident which occurs out of standard working hours e.g. leave periods and weekends.

4.4 Incident Response Coordination

4.4.1 In order to do this the Trust and individual academies will need to have a nominated Incident Response Lead.

4.4.2 In most cases for academies this will be the designated Data Champion. The Incident Response Lead for the Trust will be the Director of Governance and Data Protection Officer (DPO). Only the

DPO or Trust Incident Response Lead will determine whether the ICO, data subjects, law enforcement, insurers, legal advisers, senior leaders or governance bodies need to be notified.

4.4.3 It will be the Incident Response Lead's task to coordinate a quick, effective response to incidents, to prevent or reduce harm to individual data subjects, academies and the Trust. They will liaise directly with the DPO.

4.4.4 The Incident Response Lead, working with the Senior Leadership Team (SLT), is responsible for taking the appropriate steps they determine necessary to identify, assess, contain, mitigate and resolve the incident.

4.5 Incident response lead/Data Champion responsibilities

4.5.1 The Incident response lead/Data Champion is responsible for

- Investigating incidents and suspected breaches in a timely manner to meet the stipulated 72 hour reporting requirement.
- Assessing the severity of the incident or suspected breach, in conjunction with the academy SLT or Trust staff.
- Initiate containment and recovery action, including liaising and coordinating internal teams as required.
- Notify the DPO at the earliest possible time (in accordance with specific severity levels below) or where there is uncertainty.
- Supporting communication with data subjects where the DPO or Trust Incident Response Lead has determined that notification is required.
- Recording all data breaches.
- Conducting post breach management and evaluation supported by the DPO.

4.6 Dealing with Out-of-Hours Incidents

4.6.1 Dealing with incidents and suspected breaches out of working hours e.g. weekends and leave periods, will obviously present challenges and consideration must be given to how best these can be managed.

4.6.2 The timeline for reporting starts when someone first becomes aware of a potential breach.

4.6.3 Each academy must ensure that a nominated Incident Response Lead, deputy or other agreed contact route is available so that a response can be started without delay.

4.7 Email Address for Reporting Breaches

4.7.1 All academies will have a nominated Data Champion, all data breaches that occur within that academy will be reported directly to that member of staff using their academy email address.

4.7.2 It is the Data Champion's responsibility to nominate a deputy when they are unavailable and to ensure this is communicated to academy staff. Where the Data Champion or deputy is unavailable, or where there is any uncertainty, staff must email dataprotection@dret.co.uk without delay.

4.8 Central Trust Support and Guidance

4.8.1 Where the severity of an incident warrants escalation to the Trust, Head Office staff will support academies with advice and guidance, and assist in remedial action where appropriate.

4.8.2 This support will be coordinated by the DPO, who is authorised to draw upon Head Office functional support (e.g. IT, HR, Legal, PR) where deemed necessary to deal with any suspected breaches.

4.8.3 It is also the DPO's responsibility to report to the Trust leadership all matters pertaining to suspected severe breaches.

4.8.4 If there is any doubt as to how a suspected data breach should be dealt with, the DPO will provide advice and guidance in the first instance. The DPO's contact details below: dataprotection@dret.co.uk

4.8.5 Cover will be provided when the DPO is not available e.g. during periods of leave, prolonged illness and the DPO mailbox will be monitored by the Director of Governance.

4.9 Process for Managing Incidents

4.9.1 There are 5 steps in the process for managing incidents:

- Step 1 – Identification and Initial Assessment
- Step 2 – Containment and Recovery
- Step 3 – Risk Assessment
- Step 4 – Notification and Reporting
- Step 5 – Post Breach Management and Evaluation

4.10 Step 1 – Identification and Initial Assessment

4.10.1 Identification (Reporting) – All suspected data breach incidents, once identified, must be reported immediately to the Incident Response Lead (Academy Data Champions, DPO or nominated person) in accordance with this Data Incident Response policy.

4.10.2 Initial Assessment – Part one of the attached Data Incident Report Form (Appendix 1) should be completed at the earliest possible time by the Incident Response Lead (Data Champion or DPO). Use of the form is not compulsory, but the information it captures must still be gathered, documented and shared with the DPO where required. This enables the relevant information to be recorded consistently and communicated to key stakeholders so that they can respond appropriately. A key part of this initial assessment is considering the potential severity of the incident and whether the Trust needs to be informed at the earliest stage. The Incident Response Lead will use the completed Part one of the form, or equivalent documented information, to establish:

- The categories of personal data involved in the incident.
- The extent of the incident and its potential severity, including:
    - The categories and approximate number of individuals (Data Subjects) affected.
    - The categories and approximate number of personal data records affected.
- The cause of the incident.

- The likely consequences of the incident, including potential harm to individuals (if known)
- Any first response measures taken to deal with the incident and to mitigate the possible adverse effects (e.g. is the data encrypted?).

4.10.3 Severity – The Incident Response Lead will determine the severity of the incident or potential breach using the assessment guidance table below. Where there is any doubt as to the severity level, the DPO should be consulted at the earliest opportunity. If the severity assessment is deemed to be Level 3 or above, the incident must be escalated to the DPO immediately. Timing is essential as the ICO may need to be notified within 72 hours of the Trust becoming aware of the breach. The severity level is categorised on a scale of 1 (minor) to 5 (serious). Where incidents are rated:

- Level 1 or 2 (minor/low) they can be dealt with at academy level and DPO informed.
- Level 3 (medium) or above they must be reported directly to the DPO for evaluation.

4.10.4 Severity Assessment Guidance

Severity Level	Rating Scale	Severity Assessment (potential harm to an individual data subjects, academy and/or Trust)
1	Minor	• Breach of personal data, but no risk of harm and / or only a single data subject affected • No impact on individual or academy / Trust reputation • Data subject visibility very unlikely • No likelihood of media interest
2	Low	• Breach of personal data, but little risk of harm and / or only a limited number of data subjects affected <10 • Impact on individual or academy / Trust reputation unlikely • Data subject visibility unlikely • Media interest very unlikely
3	Medium	• Breach of personal data with risk of harm • Staff account user login details compromised • Loss of Trust IT asset (encrypted) e.g. laptop or mobile storage device • Potential impact on individual or academy / Trust reputation • Data subject visibility likely, which may require their notification • Potential for media interest and for regulatory body to be informed
4	High	• Breach of personal data with high risk of harm • Loss of Trust IT assets (unencrypted) e.g. laptop or mobile storage devices • Clear potential impact on individual, academy or Trust reputation • High expectation that Data Subjects will need to be informed • Unauthorised modifications to personal data, attacking its integrity • High potential for media interest • Regulatory body will have to be informed

Severity Level	Rating Scale	Severity Assessment (potential harm to an individual data subjects, academy and/or Trust)
5	Serious	• Breach of personal data with serious risk of harm and / or over 50 Data Subjects impacted • Actual or extremely probable impact on individual, academy or Trust reputation • Actual risk to the rights of data subjects; involving highly sensitive information; potential for ID theft. • Data Subjects will need to be informed • Media interest extremely likely • Regulatory body will have to be informed

4.11 Step 2 – Containment and Recovery

4.11.1 Once it has been established that a personal data breach has occurred the academy/Head Office must take immediate and appropriate action to contain the breach, to limit further harm or complication.

4.11.2 The Incident Response Lead at an academy will consider, in consultation with the DPO where required:

- Who needs to be informed of the incident within the wider Trust and agree with them what is required in order to contain the incident e.g. IT may be required to isolate a particular part of the academy's IT network.
- Whether the incident may be cyber-related, in which case IT must be notified immediately, affected devices or accounts should be isolated where safe to do so, passwords may need to be reset, and evidence such as suspicious emails, logs, screenshots or files must be preserved.
- Whether it would be appropriate to notify affected individual(s) e.g. if there is a high risk of serious harm/distress.
- Whether it is appropriate to inform law enforcement e.g. if a crime has been committed, such as theft.

4.11.3 In the case of the last two examples, it would be expected that the Trust/DPO will be involved due to the severity of the incident.

4.12 Step 3 - Risk Assessment

4.12.1 The Incident Response Lead is required to complete Part two (Risk Assessment) of the Data Incident Report Form. If the form is not used, the same information must be documented and made available to the DPO. This sets out a clear assessment of the incident, where relevant facts are known, to determine the proper response and to support sharing with relevant stakeholders, including the academy and Data Protection Officer. Usually, the completion of this part of the

report will follow an interview or conversation with the person reporting or responsible for the incident.

4.12.2 The assessment should consider the risk to individual data subjects:

- The type of personal data involved, how sensitive it is e.g. is it a special category of personal data such as health information?
- How many individuals' personal data was affected, which is an important factor in determining the level of risk?
- Who were the individuals affected by the incident? Were they staff, parents, students or governors? This will also be an important factor in determining the level of risk.
- Whether personal data was protected in any way, for example through encryption, password protection or remote wipe capability.
- Whether disclosed personal data could be used in a way that causes harm/distress to the individual data subject(s) e.g. breaches their privacy, causes financial loss or impacts their reputation.
- What are the potential adverse consequences to individual data subject(s)?
- How likely are those adverse consequences to materialise?
- How serious and substantial would the consequences be?

4.12.3 The assessment should also consider the risk to the academy or Trust, including:

- Parents/carers, staff and student confidence.
- Reputational harm.
- What risks could arise from damaged or deleted personal data (e.g. impact the academy's or Trust's ability to deliver a service).

4.12.4 Academies are required to keep a record of data incidents on a Data Incident Register (**Appendix 2**).

4.13 Step 4 – Notification and Reporting

Notification

4.13.1 If an incident at an academy is considered to sit within any severity level, then the academy is to inform the DPO at the earliest possible time after becoming aware of the incident, so that guidance can be sought

4.13.2 If a Data Incident Report Form has been completed, Parts 1 and 2 must be sent securely to the Trust Incident Response Lead (DPO unless directed otherwise). However, there must be no delay in notifying the DPO while the form is being completed or additional facts are being gathered; telephoning ahead can save time in the long run.

Reporting

4.13.3 Once the Trust has been notified, Part three of the Data Incident Report Form will be used by the Trust Incident Response Lead (DPO). This will be used to further evaluate the incident and determine whether external reporting of the incident is required. It will record:

- Intention to inform the ICO (the regulatory body).
- Intention to inform the Data Subjects.
- Any reporting of the incident to law enforcement agencies as deemed appropriate.
- Next steps, including any Trust level mitigation, actions required and key lessons that can be shared and cascaded across the Trust.

4.13.4 Unless the Trust Incident Response Lead (DPO) concludes that the breach is unlikely to result in a risk to individuals' rights and freedoms, it must be reported to the Information Commissioner's Office (ICO) without undue delay and, where feasible, within 72 hours of the Trust becoming aware of it. It is the responsibility of the Data Protection Officer, not individual academies, to report to the ICO as the registered Data Controller.

4.13.5 The ICO shall be told:

- Details of the breach, including the volume of data at risk, and the number and categories of data subjects.
- The contact point for any enquiries (which shall usually be the DPO).
- The likely consequences of the breach.
- Measures proposed or already taken to address the breach.

4.13.6 If the breach is likely to result in a high risk to the 'rights and freedoms' of the affected individuals then the Trust Incident Response Lead (DPO), will determine whether data subjects are to be informed of the breach. Informing data subjects will be carried out without undue delay, unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals. Academies will have the responsibility to inform parent/carers and students as directed.

4.13.7 Data subjects shall be told:

- The nature of the breach.
- Who to contact with any questions.
- Measures taken to mitigate any risks

4.14 Step 5 – Post Breach Management and Evaluation

4.14.1 The Incident Response Lead is to conduct a review of the data incident response to assess the actions taken, in conjunction with the DPO, and to identify any areas for improvement. A record of the findings of the review must be kept by academies and may be used to report periodically to the relevant academy

or Trust Board Committee to identify patterns, lessons learned and areas of weakness that need to be addressed.

4.14.2 The DPO will report to the Trust leadership the number and nature of personal data incidents, highlight key lessons and any further action, which may be required to reduce and mitigate any future risk.

5. Reporting and Consequences of Non-Compliance

5.1 Non-compliance with this policy may result in disciplinary action.

6. Policy Status

6.1 This policy does not form part of any employee's contract of employment.

7. Related Policies

7.1 This policy is related to the following other Trust policies:

- Data Protection Policy

Appendix 1: Data Incident Report Form

Part one	**To be completed by person reporting breach**
Name of person reporting incident	
Date incident was discovered	
Date and time of incident	
Place of incident	
Contact details (work email address / mobile)	
Brief description of incident (Describe what happened, the nature of the incident and how it was uncovered)	
Details of the affected personal data e.g. what classification / category of data was it? - Highly Confidential / Confidential / Internal - HR - Financial - Student data - Staff data - Special category data, as defined by GDPR[1]	
Number of individuals (Data Subjects) affected (approximate if exact figure not known)	
Location of Data Subjects affected e.g. DRET, Academies, governors	
What action has been taken to try to deal with the incident e.g. reported to police (in the case of theft) or reported to Trust IT team.	

[1] Racial or ethnic origin / Political opinions / Religious or philosophical belief / Trade union membership / Physical or mental health / Sex life or sexual orientation / Genetic data / Biometric data.

Has your line manager and / or Data Champion been informed?	
When and how was your line manager informed?	

Part two (Risk Assessment)	**To be completed by Incident Response Lead** (*Unless otherwise specified: Academy Data Champion or DPO)*
Description of the incident (Describe what happened, the nature of the incident, the time and date, and how it was uncovered)	
Details of the affected personal data e.g. what classification / category of data was it? - Highly Confidential / Confidential / Internal - HR - Financial - Student data - Staff data - Special category data, as defined by GDPR (see note 2 above)	
How much personal data was affected/lost?	
How many Data Subjects are affected?	
How will the loss adversely affect individual Data Subjects and/or the Academy/Trust	
Describe how the security of the personal data was breached, where applicable	

Can lost data be recovered	
Was the personal data protected in any way? (Were any data elements secure/encrypted in transit or at rest?)	
Severity assessment (1 (minor) to 5 (severe)) (Provide rationale for the assessment)	
Description of mitigation/action plan (Describe the intended plan to reduce any negative impact to Academy/Trust and Data Subjects or affected entities)	
Intention to notify affected Data Subjects (Describe plan for notifying affected Data Subjects) Note: notification will follow consultation with Trust Staff – the DPO in first instance.	

Part three	**To be completed by Trust Incident Response Lead** *(Unless otherwise specified: Trust DPO)*
Date and time escalated to the Trust, if severity level 3 or above	
Summary of incident Short summary to share with leadership	
Next steps Trust-level mitigation/action plan	
Intention to inform the ICO Describe decision and plan for notifying the regulator, if required	

Intention to report to law enforcement Describe decision and plan to report to police or another agency, if appropriate
Intention to inform data subjects Confirm academy/Trust plan for notifying data subjects and the means of communication
Lessons/closure Lessons learned and plans for sharing learning
Date incident closed

Appendix 2: Data incident register

To be maintained by academies and passed to DPO to record all incidents

Number	**Responsible for Notification** (name and work contact details)	**Affected Party** (e.g. Academy staff, students)	**Date Notified**	**Status** (e.g. New, ongoing, closed)

Appendix 3: what to do in the first 72 hours – checklist

Step	Checklist	Desired timeline
Step 1	**Identifying (reporting the incident)** • Incident reported to the incident response lead (Data Champion/DPO) **Initial Assessment** • Data incident report form (part 1) completed, or information gathered using the form as a guide. • Analyse the incident • Document any early stage facts and analysis • Consider the potential severity of the incident	At the earliest possible time after becoming aware of a potential breach **First 24 Hours** As soon as possible after being notified of breach
Step 2	**Containment and recovery** • Immediately contain the incident • Preserve the evidence of the incident as appropriate	**First 24 Hours** As soon as possible after being notified of the breach
Step 3	**Risk assessment** • Investigate the incident - speak to the person reporting breach to understand nature and extent of incident • Establish cause of the incident • Analyse the risks/implications of the incident • Assess the severity of the suspected breach (if initial assessment is severity level 3 or above engage the DPO at the earliest possible time. • Consider if additional support/resources required e.g. central IT support • Incident Response Lead completes Part 2 (Risk Assessment) of the Data Incident Response Form or similar.	**Within 48 Hours**
Step 4	**Notification and reporting**	**Within 72 Hours**

Step	Checklist	Desired timeline
	• Send Data Incident Report Form (Parts 1&2) to DPO if completed. • Record on Data Incident Register • Determine whether to communicate the incident to the affected individual Data Subjects (DPO to make decision) • Determine whether the ICO needs to be informed and report when deemed necessary (DPO) • Data Incident Report Form (Part 3) completed by DPO, or documented accordingly.	
Step 5	• Review incident and response, identify lessons, develop incident remediation actions • Respond to data subjects, regulators as necessary • Completed Data Incident Report Forms to be sent to the DPO (when breach managed and dealt with at Academy – severity 1 or 2) • Report to leadership as appropriate	**Post Breach** As soon as possible after 72 hour period