# Elmlea Schools' Trust

# Data Breach Policy

**Document History Record of recent Policy changes**

| Date | Version | Author/Owner | Change | Origin of Change e.g. TU request, change in legislation |
|---|---|---|---|---|
| January 2020 | 1.0 | Clare Sanders | | Appointed DPO auditwest – recommended policy. |
| January 2021 | 1.1 | Andrea Bizley | Minor: contact details updated | N/A |
| November 2022 | 2.0 | Andrea Bizley | Section 5 (SIM) merged into Section 4 | Recommended by DPO |
| November 2023 | 2.1 | Andrea Bizley | Minor change with suspected replaced by near misses | Based on DPO One West Oct 2023 template |

| | |
|---|---|
| Data Protection Officer (DPO) | i-west@bathnes.gov.uk<br>Organisation: One West (part of Bath and North East Somerset Council)<br>www.onewest.co.uk |
| Trust Data Processing Lead | Director of Finance and Operations |

| Trustees 'Committee | Audit and Risk |
|---|---|
| Policy Adopted | November 2023 |
| Review cycle | Annually<br>and when the following circumstances occur:<br>Change of Data Protection Officer,<br>Change of Legislation |
| Review date | November 2024 |

Elmlea Schools' Trust

# Data Protection – Data Breach Policy

## 1. Introduction

Elmlea Schools' Trust (EST) issues this policy to meet the requirements incumbent upon them under the Data Protection Act 2018 for the handling of personal data in its role as a data controller, such personal data is a valuable asset and needs to be suitably protected.

Appropriate measures are implemented to protect personal data from incidents (either deliberately or accidently) to avoid a data protection breach that could compromise security.

A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

## 2. Scope

This policy applies to all employees of Elmlea Schools' Trust including contract, agency and temporary staff, volunteers and employees of partner organisations working for Elmlea Schools' Trust.

## 3. Data Breaches

For the purposes of this policy data breaches will include both 'near misses' and confirmed incidents.

An incident can include, but is not limited to:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*
- Equipment failure (where this leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data)
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data *(e.g. login details, emails to the wrong recipient, not using BCC, post to the wrong address)*
- Website defacement
- Hacking attack
- Unforeseen circumstances (where this leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data) such as a fire or flood
- Human error
- Breaches of policy such as
    - Server Room door left open
    - Filing cabinets left unlocked

- Temporary loss / misplacement of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*

Near misses can include, but are not limited to, scenarios such as emails sent to the wrong recipient where a non-delivery report bounces back.

## 4. Risk Assessment and Reporting

The quick response to a suspected or actual data breach is key. When a security incident takes place, it should be quickly established whether a personal data breach has occurred and, if so, appropriate steps should be promptly taken to address it.

The focus of risk regarding breach reporting is on the potential negative consequences for individuals. On becoming aware of a breach, you should contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

All parties in scope of this policy have a responsibility to report a suspected or actual data breach. If this is discovered or occurs out of hours, this should be reported as soon as practically possible to the person responsible for the management of personal data breaches within the organisation. This should be done through the completion of the reporting form in Appendix 1, which should be sent to EST's Lead Officer who will liaise with its Data Protection Officer (One West).

Notify the ICO (if necessary) the personal data breach is likely to result in a risk to the rights and freedoms of an individual(s), the incident may need to be reported to the Information Commissioner's Office (ICO), no later than 72 hours after becoming aware of the breach. It is therefore crucial that you report any data breach (regardless of the severity) to your Data Protection Officer (DPO) as soon practically possible. It is especially important to report data breaches as promptly where there is low staff availability and or a Bank Holiday. The DPO will advise on whether to notify the ICO, however the final decision will rest with the organisation. If a decision to report is made, then it is the Organisation's responsibility to liaise with the ICO to ensure the report is sent off.

Notify data subjects (if necessary) if the breach is likely to result in a high risk to the rights and freedoms of individuals then you should promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effect of a breach. When notifying individuals, you should consider including the following:

- Outline what has occurred and apologise
- Provide name and contact details of lead officer or relevant manager for further information
- Describe any likely consequences
- Describe any measures taken or proposed to be taken to address the breach including any measures to mitigate its possible adverse effects
- Advise whether the ICO has been notified
- Record notification to the data subject in breach log.

## 5. Monitoring and compliance

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the board of trustees.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation, in consultation with the Executive Headteacher and where appropriate, the board of trustees, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

All personal data breaches (and near misses) should be recorded whether or not they have been reported to the ICO. The breach log will include the facts of the breach, its effects and the remedial action taken. Staff should be aware, that a deliberate or reckless disregard of this policy could result in disciplinary action being taken.

*Learning from experience*

The relevant manager should, in consultation with the DPO, undertake a review of existing controls to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review should consider:

- Whether policy controls are sufficient
- Whether the breach occurred due to system error or human error or both
- Whether training and awareness can be amended and/or improved (if a report to the ICO is made, they are likely to seek details of training that has been undertaken)
- Where the biggest risks are apparent and any additional mitigations
- Whether methods of transmission are secure
- If Learning from experience to be disseminated to all staff (where possible without identifying the person responsible).

## 6. Links with Other Policies

This policy should be read in conjunction with other relevant policies, including but not limited to:

- Data Protection Policy
- Information Security Policy
- Staff Acceptable Usage Policy (AUP)

## 7. Approval

This policy was approved by the Board of Trustees on 28th November 2023

# Appendix 1 – Data Incident Reporting Form

| 1. About the incident | |
|---|---|
| **Date and time of incident** | |
| **Where did the incident occur?** | |
| **Date (and time where possible) of notification to the organisation** | *If there was any delay in reporting the incident, please explain why this was* |
| **Who notified us of the incident?** | |
| **Describe the incident in as much detail as possible, including dates, what happened, when, how and why?** | *Include names of staff and data subject(s). Identifying information will be anonymised for any reporting purposes.* |
| **2. Recovery of the data** | |
| **What have you done to contain the incident?** | *eg limiting the initial damage, notifying the police of theft, providing support to affected data subjects* |
| **Please provide details of how you have recovered or attempted to recover the data, and when** | *Consider collecting the lost data, rather than relying on an unintended recipient to dispose of it* |
| **3. About the affected people (the data subjects)** | |
| **How many individuals' data has been disclosed?** | |
| **Are the affected individuals aware of the incident, and if so, what was their reaction?** | |
| **When and how were they made aware / informed?** | |
| **Have any of the affected individuals made a complaint about the incident?** | |
| **Are there any potential consequences and / or adverse effects on the individuals? What steps have been taken / planned to mitigate the effect?** | |
| **Your organisation:**<br>**Your name and contact details:** | |