Data Breach Policy and Process

Document History

Version number	4
Approved by	Board of Trustees
Approval date	June 2023
Adopted by	n/a
Adopted date	n/a
Implementation date	September 2023
Policy/document owner	Data Protection Officer
Status	Statutory
Frequency of review	Every two years
Next review date	June 2025
Applicable to	This policy applies to the Trust and all constituent schools.

Version	Date	Author	Summary of changes
V1.0	27th March 2018	Director of Operations	New draft policy – v1
V2.0	16th April 2018	Director of Operations	Revised in consultation with Director of IT
V3.0	April 2020	Head of Governance	Policy renamed from Information Security Incident Management Policy. Summarised the introduction section. Added reporting requirements in section 5.1. Included role of Lead Investigation Office in 5.2. Expanded who should be notified in section 5.3. Added section 6. Evaluation and response. Role of the Local Data Protection Officer added to Appendix 1. Other minor amendments to wording and terminology
V3.1	November 2020	Head of Governance	Updated branding
V4.0	June 2023	Data Protection Officer	Updated definition of data breach in section 3. Added GDPR Sentry as incident reporting system in section 5.1, 5.4 and Appendix 1. Added DPO as recipient of Investigation Report in section 5.3. Updated Roles and Responsibilities of DPO and Director of Operation in Appendix 1.

Contents

1. Introduction

Discovery School's Academy Trust, further referred to as **Discovery** or **the organisation** has a responsibility to ensure that data is protected.

Data security breaches will vary in impact and risk depending on the content and quantity of data involved, the circumstances of the loss and the speed of response to the incident. By managing all perceived data security breaches in a timely manner, it may be possible to contain and recover the data before it an actual breach occurs, reducing the risks and impact to both individuals and the Trust.

2. Purpose

The purpose of this policy is to provide guidance on how data breaches should be handled and reported and to identify the roles and responsibilities of key personnel in the investigation of such incidents. The aim of this document is to ensure that relevant and prompt action is taken on actual or suspected data breaches to minimise their impact and the risk of recurrence.

3. Scope

The policy applies to:

- Discovery colleagues, contractors, partners and suppliers.

A data breach can broadly be defined as a security incident that has affected the confidentiality, integrity and availability of personal data. There is a data breach whenever personal data is accidently lost, destroyed, corrupted or disclosed; if someone else accesses the data, or passes it on without proper authorisation, or if the data is made unavailable and this unavailability has a significant negative effect on individuals. Examples of a data breach are the following: -

- The loss or unauthorised disclosure of personal or sensitive information.
- Transfer of personal and sensitive information to those who have no need to see it.
- Attempts (failed or successful) to gain unauthorised access to information or a computer system.
- Unauthorised changes to information or system hardware/software.
- Loss or theft of ICT equipment including peripheral storage items
- Unauthorised use of a system (electronic or manual) for processing/ storage of data by any person.

4. Roles and responsibilities

Appendix 1 highlights the key roles and responsibilities for managing data breaches within the organisation.

5. Data Breach Process

The Data Breach Process is detailed below and illustrated in **Appendix 3**.

5.1 Incident Reporting

Reports of a data breach may come from an internal or external source.

Any individual who accesses, uses or manages the organisation's information is responsible for reporting an actual or suspected data breach immediately to their Local Data Protection Officer.

The Local Data Protection Officer will report the incident and complete a Data Breach assessment on our GDPR Sentry software within 24 hours of the incident so that the incident can be further investigated. The Data Protection Officer (**DPO**) will be notified as soon as the incident is put onto GDPR Sentry.

Incidents related to IT, e.g. an actual or suspected technical attack on systems or the loss of IT equipment, will be notified by the DPO to the Director of ICT.

All staff should be aware that any breach of Data Protection legislation may result in disciplinary procedures being instigated.

5.2 Investigation

An initial assessment will be made by the DPO to establish the severity of the breach – Appendix 2 . Where it is determined that further investigation is warranted a Lead Investigation Officer will be appointed, this will depend on the nature of the breach and in some cases, it could be the DPO.

The Lead Investigation Officer (LIO) will:

- Establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.
- Ensure that personnel with the appropriate knowledge and technical expertise are involved where there is a requirement for retrieval of information or recovery of systems/ equipment.
- Determine whether there are any third parties involved or affected by the incident e.g. other authorities, suppliers etc and decide whether they need to be notified or not.
- In liaison with the DoO/DPO determine the suitable course of action to be taken to resolve the incident
- Prepare an investigation report for review by the DoO/DPO and escalation to the Trust Leader and Board of Trustees where relevant.
- Liaise with HR to consider whether an investigation under the disciplinary procedure is appropriate and required.

5.3 Notification

Where an incident is deemed to be serious, this would need to be reported to the Trust Leader and the Board of Trustees.

The LIO in consultation with the DPO and DoO will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred, and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks.

The LIO and the DoO/DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

5.4 Incident log

A record will be kept of any incident, regardless of whether notification was required. A Data Breach log is updated and maintained by each school on the GDPR Sentry system. The DPO will use this log to look for trend analysis. The log categorises incidents to enable meaningful reporting.

6. Evaluation and response

Once the initial incident is contained, the **DPO** will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;
- staff awareness.

7. Policy review

This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation. A formal review will be completed every three years.

This policy was last reviewed in June 2023. The policy was approved Board of Trustees in [put approval date in].

Appendix 1: Roles and Responsibilities

Role	Responsibilities
All employees	• Comply with Discovery policy and legal requirements relating to information security and GDPR regulations. • Report any incidents/ potential incidents likely to cause a breach of the organisation's policies and/or legislation. • Raise any unusual security-related occurrences with their relevant line manager. • Contribute to investigations as and when required. • Ensure evidence of an information breach is not damaged.
Headteacher & Exec team for ATSA/SCITT/EPIC/DSAT	• Accountable for ensuring all staff they are responsible for are aware of the Data Breach Policy Process. • Implement controls as suggested in order to prevent/minimise the risk of incidents reoccurring. • Review and amend policies and procedures to reduce the risk of incidents occurring • Seek security advice from DoO and the Director of IT where required • Ensure all other relevant stakeholders are kept informed throughout the incident process • Liaise with central HR to determine if an investigation under the disciplinary procedure is required.
Local Data Protection Officer This is usually the Office Manager	• Ensure all staff are aware of the Data Breach Policy and Process locally. • In the event of an incident, notify the Headteacher or relevant senior leader and formally report (via GDPR Sentry system). • Manage the data breach process and contribute to the investigation • Maintain the data breach log of the incident on GDPR Sentry. • Keep stakeholders informed throughout the process as required. • Update the Headteacher/relevant senior leader.
Lead Investigation Officer (LIO)	• Undertake the investigation • Complete an incident report for submission to the DoO/DPO • Involve key stakeholders in the investigation as and when required and keep them informed • Seek advice from specialist areas where required
ICT Services	• Monitor technical facilities to detect potential security incidents. • Implement the Incident Process or Major Incident Process if warranted by the incident. • Conduct technical investigations and recovery of information systems following a data breach. • Regularly review procedures and technical configurations to reduce the risk of incidents occurring. • Implement controls as recommended. • Communicate any system down time/ issues to users.
DPO	• Co-ordinate/undertake investigation when required. • Provide advice to the nominated officer undertaking the investigation if not DPO. • Keep the incident log up to date and track the tasks delegated to officers. • Keep all other relevant stakeholders informed throughout the incident process. • Where applicable, report incidents to the Information Commissioner's Office.

	• Ensure follow up actions from incidents are being completed • Regularly review and update this policy • Advise on mitigating controls that can be implemented to prevent reoccurrence of incidents • Provide advice on the data breach process and ensure relevant documentation is completed in the event of an incident • Provide support to relevant stakeholders as appropriate during investigations. • Share best practice. • Undertake reviews to ensure controls are working as intended.
Central HR / Legal	• Support managers on any HR/legal issues when undertaking investigations. • Liaise with key stakeholders as appropriate during investigations. • Work with DoO and DPO to help improve controls, policies, and procedures.
Director of Operations	• Be made aware of incidents, outcomes, and recommendations. • Co-ordinate/undertake investigation when required. • Assist DPO in any on-going investigations or incidents • Support DPO in ensuring follow up actions from incidents are being completed • Share best practice
Trust Leader	• Be made aware of incidents, outcomes, and recommendations. • Obtain assurances that follow up actions are carried out. • Acts as appropriate on issues encountered within investigations or in implementing remedial recommendations. • Authorise the reporting to the Information Commissioner where required
Board of Trustees	• Receives a summarised list of incidents, outcomes, and recommendations for scrutiny • Approve the Data Breach Policy and Process • Be made aware of serious incidents, their outcomes, recommendations, and completion of actions where there is a possible requirement to report to the ICO

Appendix 2: Severity Table

NB: This table only gives broad guidelines on the severity of incidents. Each case may differ depending on other variables e.g., the number of people affected, the type of information concerned etc. The severity of each incident should therefore be considered on an individual basis.

Incident Type	**Breach of** (Confidentiality, Integrity, Availability & Accountability)	**Severity**
Unauthorised access to Network/ Systems/ Applications/ Email	Integrity/ Confidentiality/ Availability & Accountability	Moderate to Major depending on the level of information accessed
Sending information		
Information sent to the wrong recipient (internally), disclosing information that is neither confidential not personal	Integrity	Minor
Information sent to various recipients (including external recipients) disclosing non confidential or non-personal information	Integrity	Moderate
Information sent to an unauthorised recipient(s) containing confidential and sensitive personal information (whether Internal or External)	Integrity/Confidentiality	Major
Loss of equipment		
Loss or theft of equipment containing no confidential and/or personal information	Availability	Minor/ Moderate
Loss and theft of equipment containing confidential and/or personal information but with encryption software installed on the equipment	Availability/ Confidentiality	Moderate
Loss and theft of equipment containing confidential and/or sensitive personal information where equipment has no encryption software installed	Availability/ Confidentiality	Major
Inappropriate material found on PC	Accountability	Minor to Major depending on the type of material found on the PC
Illegal material found on PC	Accountability	Major
Inappropriate/unauthorised use of the network/software leading to a disruption of services	Availability	Major
Inappropriate use of the internet or email as defined within the AUP Policy	Accountability/ Availability	Minor to Major depending on the circumstances
Passwords written down leading to unauthorised access	Integrity/ Confidentiality/ Availability & Accountability	Moderate/ Major depending on the type of information and system and impact of the incident
Offensive emails being sent	Accountability	Moderate to Major depending on content of the email
Spam or 'phishing' emails	Availability	Minor to Moderate depending on the impact and number of users affected.
Information sent externally or internally by fax, post or hand (containing no confidential or personal information) is lost	Availability	Moderate

Information sent externally or internally by fax, post or hand (containing confidential or sensitive personal information) is lost	Integrity/ Confidentiality/ Availability & Accountability	Major
Unintentional corruption of data	Availability	Moderate/Major depending on the amount of data and type of data corrupted
Intentional corruption of data	Availability and Accountability	Major
Password sharing	Accountability/ Integrity/ Confidentiality	Moderate to Major depending the type of data in question
Downloading or copying of unlicensed software	Accountability	Major
Information/ data deleted or amended from a database in error	Accountability/ Integrity & Availability	Moderate
Information/ data deleted or amended from a database maliciously	Accountability/ Integrity & Availability	Major
Confidential information disposed of inappropriately	Accountability	Major
Website Hacked	Availability/ Integrity	Moderate to Major depending on the criticality of the system
Misuse of Telephony Service	Accountability	Minor to Major on the level of misuse

Appendix 3: Data Breach Process diagram