Northern School of Contemporary Dance

Data Breach Policy and Procedure

Policy owner:	Northern School of Contemporary Dance: Leadership Team
Lead contact:	Information Systems Manager
Audience:	Applicants/Students/Staff/partners for Northern School of Contemporary Dance
Approving body:	Northern School of Contemporary Dance: Audit Committee
Date approved:	November 2025
Policy Implementation date:	November 2025
Supersedes:	N/A
Previous approved version(s) dates:	N/A
Review cycle:	Two yearly
Next review due date:	November 2027
Related Statutes, Ordinances, General Regulations	UK GDPR & Data Protection Act (2018)
Related Policies, Procedures and Guidance:	Student Complaints, Staff Complaints, Public Complaints, Data Protection Policy
UK Quality Code reference:	
OfS Conditions reference:	Conditions E: Management & Governance, B3: Student Outcomes & Experience
Equality and Diversity Considerations:	Policy should be available in accessible format for all students.
Date Equality and Diversity Assessment Completed:	N/A
Further information: Policy reviewed by the Data Compliance Sub-Committee April 2025	

Data Breach Policy

1. Introduction

This policy aims to outline our commitment to implementing a data breach process for the handling of data breaches and other data affecting processes.

Data security breaches are increasingly common occurrences whether caused through human error or via malicious intent. As the amount of data and information grows and technology develops, there are new ways by which data can be breached.

NSCD needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect personal data which it holds.

2. Scope & Principles

The policy applies to all processes relating to activities of NSCD handling data, in electronic or physical form, and is applicable to all those who engage with NSCD including; governors, students, staff including permanent or temporary contractors and others employed under a contract of service and visitors.

It applies to all conduct of NSCD including activities outside of NSCD that is related to its activities.

The aim of this policy is to standardise NSCD's response to any data breach and ensure that they are appropriately logged and managed in accordance with the law and best practice, so that:

- incidents are reported swiftly and can be properly investigated
- incidents are dealt with in a timely manner and normal operations restored
- incidents are recorded and documented
- the impact of the incident is understood, and action is taken to prevent further damage
- the ICO and data subjects are informed as required in more serious cases
- incidents are reviewed, and lessons learned

3. Definitions

Article 4 (12) of the General data protection Regulation ("GDPR") defines a **data breach** as:

> ***"a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."***

NSCD is obliged under the GDPR to act in respect of such data breaches. This procedure sets out how NSCD will manage a report of a suspected data security breach.

The aim is to ensure that where data is misdirected, lost, hacked or stolen, inappropriately accessed or damaged, the incident is properly investigated and reported, and any necessary action is taken to rectify the situation.

A data security breach can come in many forms, but the most common are as follows:

- Loss or theft of paper or other hard copy
- Data posted, emailed or faxed to the incorrect recipient
- Loss or theft of equipment on which data is stored
- inappropriate sharing or dissemination-Staff accessing information to which they are not entitled
- Hacking, malware, data corruption
- Information is obtained by deception or “blagging”
- Equipment failure, fire or flood
- Unescorted visitors accessing data
- Non-secure disposal of data

In any situation where staff are uncertain whether an incident constitutes a breach of security, either report it to the Privacy Officer (PO). If there are IT issues, such as the security of the network being compromised, IT should be informed immediately.

4. Responsibilities

All members of NSCD have a responsibility to abide by and promote the principles in this policy in relation to their work and duties at NSCD. The policy must be known, understood, and implemented.

The procedure is applied objectively without judgement.

Information users

The GDPR applies to both Data Controllers and to Data Processors. Therefore, all information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

Managers

Managers are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

Lead Responsible Officers

Lead responsible officers (PO) will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. Suitable further delegation may be appropriate in some circumstances. The PO for NSCD is the Information Systems Manager.

4.1 The Data Compliance Sub-Committee will be responsible for:

- Overseeing the continuing application and development of the Data Breach policy in line with legislation and strategic objectives
- Overseeing the formation and implementation of
- Collating and analysing appropriate monitoring data
- Report on to Senate and the Audit Committee

4.2 The CEO/Principal will be responsible for ensuring the Data Compliance Sub-Committee regularly review the policy and apply it appropriately.

4.3 The Board of Governors will be responsible for delegating the monitoring of the use of the policy to the Audit Committee.

5. Communication of Policy

This policy will be published in the Quality Office policies channel and school public website.

NSCD will endeavour to provide documents in different formats if requested by applicants, staff and students.

The induction of all staff will include specific reference to the Policy and the responsibility of staff to reflect its principles in their own practice.

6. Legal Framework

This policy has been enacted to comply with the **Data Protection Act (2018).** Organisations are required to handle data breaches and inform the Information Commissioners Office (ICO) of data breaches with 72 hours of them occurring.

Article 33 of the GDPR requires NSCD as data controller to **notify the ICO** only when the breach "is likely to result in a risk to the freedoms and rights of natural persons". Such a breach also must be communicated to the data subject (with certain exceptions).

Notification must be made "without undue delay" and **within 72 hours** of becoming aware of it. If NSCD fails to do this, it must explain the reason for the delay.

Article 33(5) requires that NSCD must **maintain documentation** on data breaches, their nature and remedial action taken.

A report to the ICO must contain information as to the nature of the breach, categories of data, number of data records, number of people affected, name and contact details of PO, likely consequences of the breach and action taken.

7. Breach of the Policy

Northern School of Contemporary Dance will take seriously any instances of infringement of the Data Breach Policy by students, staff, users or participants.

Any instances of infringement will be investigated and where appropriate will be considered under the relevant complaints/grievance and disciplinary policy for staff or students.

8. Complaints

Staff, students or visitors who wish to make a complaint regarding the Data Breach policy should seek resolution through the complaints procedure if unable to be resolved through informal means.

Student Complaints Policy & Procedures
Staff Complaints Policy & Procedures
Public Complaints Procedure

9. Key contacts

Name	Role	Email
Information Systems Manager	Policy Oversight / Data Protection Officer	Glenn.glidden@nscd.ac.uk
Student Services	Student Support or general enquiries	studentservices@nscd.ac.uk

10. Data Breach Procedure

10.1 Overview

This process document details how NSCD will deal with the notification of a data breach and its investigation. It also deals with how NSCD deal with data issues notifications, e.g. weaknesses in software requiring patching, or suspicious activity to look out for. For the purposes of this document, the term data breach will be used but includes data issues.

10.2 Procedure

NSCD's response to any reported data breach will involve the following four elements.

- Containment and Recovery
- Assessment of Risks
- Consideration of Further Notification
- Evaluation and Response

Each of these four elements will need to be conducted in accordance with the checklist. An activity log recording the timeline of the incident management should also be completed.

NB. This reflects current guidance from the ICO, which is likely to change.

10.3 Notifications of Breaches

The Information Systems Manager (ISM) needs to get notification of a breach if it is to be progressed.

10.4 Externally Raised

Externally raised breaches come in from various sources. The School gets it's internet provision from JISC and as such has security channels with them for the reporting and notification of breaches and/or issues. Additionally the ISM is a member of the National Cyber Security Centre and gets notifications from them. Finally, we may get notified of breaches through other channels, such as our email and anti-virus systems, or Microsoft monthly patch alerts.

10.5 Internally Raised

Staff are advised to notify the dataprotection@nscd.ac.uk email address of any suspected breach. They will then be asked to complete an initial form to collate relevant data.

The ISM and IT technician will also self-raise issues to look at.

10.6 Initial Review

The Information Systems Manager (ISM) will do an initial review of the breach to consider initial steps.

Once that initial review has been completed, the ISM will discuss with a Leadership Team (LT) member their conclusion as to how it needs to be approached. There are three levels that could apply;

1) The ISM handles the issue directly (e.g. software patching notifications) and records the event in the log.
2) The ISM convenes a Data Compliance Sub-Committee sub-group to assess the issue.
3) The ISM go straight to an investigation/remediation cycle, notifying the DCSC and LT of the event, as well as the Clerk to the Governors.

10.7 Data Compliance Sub-Committee Sub-Group Review

If necessary, the ISM will convene a sub-group of the DCSC to review the breach.

This group will consist of the ISM, a member of the LT for the area affected, and a department head for the area affected.

For example if the data breach primarily affected student data, the constituents would be the ISM, Director of Higher Education and the Head of Registry.

The review will assess if it is an actual data breach (i.e. potentially reportable to the Information Commissioners Office (ICO)), or a breakdown of internal processes.

In the event of an obvious data breach, review group will be informed that a formal data breach process is being started.

10.8 Investigation Processes

The investigation process will differ depending on the type of data breach.

10.9 Suspected Breach

In the event of a suspected breach, the ISM will investigate the breach using the case summary document. This details the work completed, who was interviewed and the statements that were made.

Initially the reporting person is asked to complete a reporting template to gather the primary information about the breach.

Any actions taken by the school to contain the breach will be logged.

Once the investigation is completed, the ISM and the sub-group will convene to review the breach and implement next steps. This will include if a report to the ICO is required, and/or is a reportable issue for the OfS to be aware of.

10.10 Breakdown of Processes

In the event of a process breakdown, the ISM will convene a meeting of the affected parties to discuss the issue and set some action points for the re-enforcement or revision of the processes.

Note that the same remediation processes will need to be carried out to correct the breakdown of process.

10.11 Further Internal Actions

It is noted that this process is a research and remediation process. Should that process yield possible capability or disciplinary processes, that would need to be determined and actioned outside of this process.

10.12 Formally Reporting Breaches

Breaches and issues are logged by the ISM. These breaches/issues are reported on an annual (calendar based) report to the NSCD Audit Committee.

Note a summary of data actions (Data Breaches, FOI Requests and Data Subject Access requests) will also be collated in summary form as an annual report of activity.

Where necessary, formal notifications will be made to the ICO and/or OfS using their reporting processes.