Personal Data Breach Procedure

1. Background

The National Film and Television School ('the School') is committed to a policy of protecting individuals' right to privacy in accordance with the General Data Protection Regulation ((EU) 2016/679) (the GDPR) and the Data Protection Act 2018 (the DPA). This document sets out the guidance and procedure for personal data breach incidents at the School and must be read in conjunction with the School's Data Protection Policy.

The School is required to take appropriate measures against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

The GDPR requires the School to report all personal data breaches (except those which are "*unlikely to result in a risk to the rights and freedoms of natural persons*") to the Information Commissioner's Office within 72 hours of becoming aware of the breach, and to maintain a log of all breaches. Failure to comply with the GDPR can lead to enforcement actions, including fines of up to €20 million or, if higher, 4% of an organization's annual turnover. It is therefore crucial that the School has a robust breach detection, investigation and internal reporting procedure in place.

This procedure applies to School staff, agency workers, students, volunteers, contractors and third party agents who process data for or on behalf of the School and it must be complied with in the event of a data security breach.

2. What is a personal data breach?

The GDPR defines a **personal data breach** *as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

Personal data is any information relating to an identified or identifiable individual; an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

A personal data breach can happen for a number of reasons. In general terms, a breach will occur whenever any personal data is lost, destroyed, corrupted or disclosed. Data breaches can fall into three categories:

(1) "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.

(2) "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

(3) “Availability breach” - where there is an accidental or unauthorised loss of access to, or destruction of, personal data

Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. loss or theft of a computer, portable device, such as a laptop or data stick)
- Unauthorised access to, use, or alteration of personal data
- Deliberate or accidental action (or inaction)
- Loss of availability of personal data (e.g. encrypted by ransomware, or accidentally lost or destroyed) or through equipment failure (e.g. data cannot be accessed and is not backed up)
- Human error (e.g. sending data to the wrong recipient or accidentally deleting it)
- ‘Phishing’ offences where information is obtained by a third party through deception.

3. What should I do when a breach occurs?

Any individual who accesses, uses or manages the School’s information is responsible for reporting a personal data breach and information security incidents **immediately** to the Data Protection Officer (at DPO@nfts.co.uk) and Director of Operations (at mtugwell@nfts.co.uk). If the breach occurs or is discovered outside normal working hours, it must be reported **as soon as is practicable**.

If you know or suspect a personal data breach has occurred you should IMMEDIATELY:

- complete a data breach report form, as set out in Appendix 1. You can download a copy of the form from Facebook Workplace.
- email or deliver the completed form to mtugwell@nfts.co.uk and DPO@nfts.co.uk.

[additional info]The Director of Operations will deal with the breach. In his/her absence a breach report will be dealt with by another Director of the School. Once a report form has been submitted and receipt of the report has been acknowledged, you should take NO FURTHER ACTION in relation to the breach unless specifically asked to do so.

Set out below is a guide to the procedure that the Director of Operations will follow when he/she is made aware of a personal data breach.

4. On discovery of a breach

If the breach is a continuing breach, steps must be taken immediately to minimise the effect of the breach, e.g. to shut down a system or alert relevant staff.

Following receipt of a report of a suspected breach the DPO and Director of Operations will confirm whether a breach has occurred and assess the risks associated with it. They will ask the person reporting the breach to provide full and accurate details of the incident, when the breach occurred (dates and times), if the data relates to people, the nature of the information, and how many individuals are involved.

All staff should be aware that any breach of the Data Protection Act may result in the School's Disciplinary Procedures being instigated.

An initial evaluation will be made by the DPO and Director of Operations in liaison with relevant School staff to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach in some cases it could be the Director of Operations or another Director).

The evaluation of the breach will include an assessment of:

- the type of data involved
- its sensitivity
- the protections which are in place (e.g. encryptions)
- what has happened to the data (e.g. has it been lost or stolen)
- whether the data could be put to any illegal or inappropriate use
- who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach

The person leading the investigation will contact the Director or Head of the relevant area to explain:

- the nature of the breach
- an indication of the seriousness of the breach
- any action the School or Service must take immediately

  (i) to contain the breach and

  (ii) to become compliant with the GDPR/DPA and/or

  (iii) to prevent a similar situation from arising in the future.

The DPO and Director of Operations will continue to monitor the situation to ensure that the department responsible for the breach completes any required actions as soon as possible.

5. Managing the consequences of a breach

Depending on the seriousness of the breach and following guidance issued by the Information Commissioner's Office (https://ico.org.uk/for-organisations/guide-to-the-

general-data-protection-regulation-gdpr/personal-data-breaches/). The DPO may advise on what further steps should be taken, which may include:

- informing the School's Director
- informing the Information Commissioner's Office (this is mandatory where there is a risk to people's rights and freedoms)
- informing the Director of Marketing and External Relations if there is potential for press interest
- informing the data subjects affected by the breach.

6. Record keeping

The School maintains a Personal Data Breach Register to record details of all breaches. This record is maintained by the DPO.

7. Preventing a repetition of a breach

After completing the procedures set out above, the DPO will evaluate the breach and the effectiveness of the School's response to it.

The DPO will consider any changes that may be required to be made to School policies and procedures to prevent a breach from recurring.

This procedure was last approved and updated in May 2018

Appendix 1:

Personal data breach report form

If you know or suspect a personal data breach has occurred, please:

- complete this form, and
- email or deliver it to mtugwell@NFTS.co.uk and DPO@NFTS.co.uk , ensuring you mark your email or the form as urgent

Date of this report	
Name and contact details	
Dept/manager	
Date breach took place (if known)	
Date of discovery	
Summary of the facts: What happened? What data was affected? How many individuals were affected? Are they colleagues, contacts or members of the public? What data is affected?	
Cause of the breach	
Is the breach ongoing?	