National Film and Television School (the "School")
Data Protection Policy

1. Purpose and scope

The purpose of this policy is to ensure compliance with the Data Protection Legislation[1]. It sets out the responsibilities of the School, its staff and students to comply fully with the Data Protection Legislation.

Data Protection Legislation applies to the storing or handling ('processing') of information ('personal data') about living identifiable individual (data subjects'). It applies to personal data held in electronic format, and in paper records where these records are held in a "relevant filing system", i.e. a sufficiently structured and searchable filing system, such as a filing cabinet or organized records room. It also applies to personal data held visually, for example, in photographs or video clips (including CCTV) or as sound recordings

This policy applies to all students and staff, and all items of personal data that are created, collected, stored and/or processed through any activity of the School across all areas including departments and professional services. In this policy 'staff' means anyone working in any context within the School and whether permanent, fixed term or temporary, and including visiting tutors, interns, volunteers, agency staff, workers, and external members of committees or Boards.

This policy should be read in conjunction with:

(a) the obligations set out in staff employment contracts and worker agreements which impose confidentiality obligations in respect of information held by the School

(b) information security policies, procedures, and terms and conditions

(c) the Records Management and Retention Policy, and

(d) any other contractual obligations on the School or individual staff or students which impose confidentiality or data management obligations in respect of information held by the School.

[1] This comprises the UK General Data Protection Regulation and the Data Protection Act 2018

2. Introduction

The School is committed to complying with the Data Protection Legislation as part of everyday work practices. This includes but is not limited to understanding and applying the data protection principles; understanding and fulfilling the rights given to data subjects under the Data Protection Legislation; and understanding and implementing the School's accountability obligations under the Data Protection Legislation.

The School is a registered data controller under the Data Protection Legislation The School maintains a data protection notification with the Information Commissioner (the independent authority responsible for overseeing compliance with the data Protection Legislation) which means that the Information Commission is notified of the types of personal data processed by the School, the purposes for which the School processes data and whether or not the School transfers personal data outside the European Economic Area. The School's register entry number with the Information Commissioner's Office is Z6441288.

The School collects and processes personal data about employees, students, alumni and other individuals (collectively "data subjects") for academic, administrative and commercial purposes. This Data Protection Policy applies to all personal data the School holds about data subjects, whatever its source.

"Processing" means virtually any dealing with personal data, such as obtaining, accessing, recording, holding, disclosing, destroying or using the data in any way. The School will usually only process a data subject's personal data where the data subject has given his/her consent or where processing is necessary to comply with the School's legal obligations. In other cases, processing may be necessary for the performance of a contract with the data subject, for the School's legitimate interests or the legitimate interests of others.

The School will only process 'special categories' of personal data (for example, information relating to ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life, criminal proceedings or convictions) when a further condition is met (for example, the data subject has given his/her explicit consent, or that the processing is legally required for employment purposes).

3. Data protection roles and responsibilities

The School's Data Protection Officer is the Registrar.

The NFTS is the Data Controller under the Data Protection Legislation.

4. Data protection principles

The School strives to comply with data protection principles outlined in Data Protection Legislation when processing personal data. The School has practices and procedures in place to ensure that personal data is:

(a) processed fairly and lawfully and in a transparent manner,

(b) collected for a specified, explicit and legitimate purpose and shall not be processed in any manner incompatible with those purposes,

(c) adequate, relevant and not excessive for the purpose for which it is processed,

(d) kept accurate and where necessary up-to-date,

(e) not kept for longer than necessary for the purpose,

(f) processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures.

5. Data the School collects and the conditions of processing

In order for it to be legal and appropriate for the School to process personal data, at least one of the following conditions must be met:

(a) The data subject has given his or her consent

(b) The processing is required due to a contract

(c) It is necessary due to a legal obligation

(d) It is necessary to protect someone's vital interests (i.e. life or death situation)

(e) It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

(f) It is necessary for the legitimate interests of the controller or a third party and does not interfere with the rights and freedoms of the data subject.

All processing of personal data carried out by the School meets one or more of the conditions above.

5.1 Employees

An employee's personnel file will contain information about his/her work history with the School and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal and personal information about the employee including address details and National Insurance number. This information is collected to monitor an

employee's progress in their work and to enable the School to contact the employee when necessary.

There may also be other information about the employee located within the organization, for example, in his/her manager's email inbox or computer desktop; or within documents stored in a "relevant filing system".

5.2 Students

A student's file will contain information about his/her history with the School and may, for example, include application forms, assessment forms, references, progress reviews, absence records, and personal information about the student including address details. This information is collected to monitor a student's academic progress and to enable the School to contact the student when necessary.

There may also be other information about the student located within the organization e.g. in NFTS email folders or other electronic storage; or within documents stored in a "relevant filing system".

5.3 Employees' and students' special category personal data

The School may collect relevant special category personal data from employees and/or from students for equal opportunities monitoring and other (for example, HESA – see below) monitoring purposes. Where such information is collected, the School will only use it for such monitoring purposes unless there is a need to process it for a further purpose. If the information is to be used for a further purpose, the School will inform employees and/or students (as applicable) on any monitoring questionnaire of the further purpose for processing, the individuals (identified by name or by role) or departments within the School who will have access to that information and the security measures that the School will put in place to ensure that there is no unauthorized access to it.

The School will ensure that personal information about an employee/a student, including information in employee/student files, is securely retained. The organization will keep hard copies of information in secure filing cabinets or equivalent secure storage. Information stored electronically will be subject to access controls (including username and password based login details) and encryption software may be used to protect the data 'at rest'.

6. Rights to Access Personal Data

The Data Protection Legislation gives data subjects the right to access personal information held about them by the School. The purpose of a subject access request is to allow individuals to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary. However, individuals

can request to see any information that the School holds about them which includes copies of email correspondence referring to them or opinions expressed about them.

The School must respond to all requests for personal information within one month and information will normally be provided free of charge.

References are disclosable to the person about whom they are written under the subject access provisions of the Data Protection Legislation. This includes references received by the School from external sources. There is an exemption from disclosure for references written by School staff and sent externally, however these references would still be accessible to the applicant from the organisation to which the reference was sent. In order to maintain confidentiality and to prevent the unauthorised disclosure of information, staff should not provide references without a prior request from the student concerned.

The School is not required to disclose examinations scripts; however, students are entitled to access any marks or comments annotated on the script. Students are entitled to their marks for both coursework and examinations. Unpublished marks must be disclosed within 5 months of a subject access request.

For information about making a subject access request, see the School's Data Access Procedure.

7. Data Subject's Rights

Data subjects have a number of other rights under the Data Protection Legislation. These include:

7.1 Right to object

Data subjects have the right to object to specific types of processing which includes processing for direct marketing. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation, except in the case of direct marketing where it is an absolute right. Online services must offer an automated method of objecting. In some cases, there may be an exemption to this right for research or statistical purposes done in the public interest.

7.2 Right to be forgotten (erasure)

Individuals have the right to ask the School to erase their data in certain situations such as where the data are no longer required for the purpose for which they were collected, the individual withdraws consent or the information is being processed unlawfully. Individuals can ask the controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved or the processing is unlawful.

7.3 Rights in relation to automated decision making and profiling

The right relates to automated decisions or profiling that could result in significant affects to an individual. The School does not carry out automated decision making or profiling.

7.4 Right to rectification

The right to require the School to rectify inaccuracies in personal data held about them. In some circumstances, if personal data are incomplete, an individual can require the School to complete the data, or to record a supplementary statement.

7.5 Right to Portability

The data subject has the right to request information about them is provided in a structured, commonly used and machine-readable form so it can be sent to another data controller. This only applies to personal data that is processed by automated means (not paper records); to personal data which the data subject has provided to the controller, and only when it is being processed on the basis of consent or a contract.

If you are a student and you wish to exercise any of the rights above, please contact the Registry Manager (Registry@nfts.co.uk)

If you are an employee and you wish to exercise any of the rights above, please contact the HR Advisor (HR@nfts.co.uk)

8. Providing Information to Third Parties

The School may share a data subject's personal data with selected third parties if:

(a) the third party is providing a useful or essential service to the data subject, for example the (outsourced) payroll provider and pension advisors;

(b) the School is under a under a duty to disclose or share personal data in order to comply any legal obligation; or

(c) it is necessary to protect the School's rights, property or safety of any third party.

In particular, the School will send some of the student information we hold to the Higher Education Statistics Agency ("HESA"). HESA collects and is responsible for the database in which HESA student records are stored.

Details of how HESA will process this information can be found at:

https://www.hesa.ac.uk/about/regulation/data-protection/notices.

The School will not otherwise disclose a data subject's personal data to a third party without his/her consent. Where the School does disclose a data subject's personal data to a third party, the School will have regard to the data protection principles as described above.

Personal data will only be transferred outside the EU under certain circumstances. The School will ensure that appropriate safeguards are in place to protect the data and that the rights of data subjects are available in respect of it.

9. Monitoring

The School's systems enable it to monitor telephone, email, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in its role as an employer, use of the School's systems, including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

A CCTV system monitors the exterior of the building, Reception, Ossie Morris Canteen, Rose Building Café and behind the bar. This data is recorded.

In exceptional circumstances, the School may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to the School by the activity being monitored and where the information cannot be effectively obtained by a less intrusive means (for example, where an employee is suspected of stealing property belonging to the School). Covert monitoring will take place only with the approval of the School Director on the recommendation by the Registrar or HR Director.

The School reserves the right to retrieve the contents of email messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (the list is not exhaustive):

(a) To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy;

(b) To find lost messages or retrieve messages lost due to computer failure;

(c) To assist in the investigation of alleged wrongdoing;

(d) To comply with any legal obligation.

10. Retention of Data

The School will keep different types of personal data for differing lengths of time, depending on legal, academic and operational requirements, and legal and regulatory requirements and sector good practice. The School will not keep personal data for longer than necessary.

11. Training

The School provides training on data protection to all employees handling personal data in the course of their duties at work.

12. Personal Data breach

The School is responsible for ensuring appropriate and proportionate security for the personal data that we hold. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The School makes every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions. Examples of personal data breaches include:

(a) Loss or theft of data or equipment

(b) Inappropriate access controls allowing unauthorised use

(c) Equipment failure

(d) Unauthorised disclosure (e.g. email sent to the incorrect recipient)

(e) Human error

(f) Hacking attack

If a data protection breach occurs the School is required in most circumstances to report this as soon as possible to the Information Commissioner's Office, and not later than 72 hours after becoming aware of it.

If you become aware of a data protection breach it must be reported immediately. Details of how to report a breach and the information that will be required are included in the Personal Data Breach Procedure.

All staff and students of the School are required to comply with this Data Protection Policy. Any member of staff or student who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy may be subject to disciplinary action.

Any questions or concerns about the interpretation or operation of this Data Protection Policy should be directed to dataprotection@nfts.co.uk

This policy was last approved and updated in September 2021