Portable Device and Removable Media Usage Policy

Organisation	National Film and Television School
Title	Portable Device Acceptable Use Policy
Creator	Head of IT
Approvals Required	1. Head of IT 2. Management Team
Version	1.3
Owner	Head of IT
Subject	The formal, approved, Portable Acceptable Use Policy of NFTS
Rights	Public
Review date and responsibility	Annually by Head of IT

Document Amendment History		
V0.2	Incorporating management feedback – in particular policy application	March 2017
v1.0	Finalising policy following Management Team meeting 4/4/2017	April 2017
V1.1	GDPR update and annual review	Sept 2018
V1.2	Added Electronic File Transfer elements	August 2020
V1.3	Annual Review	March 2023

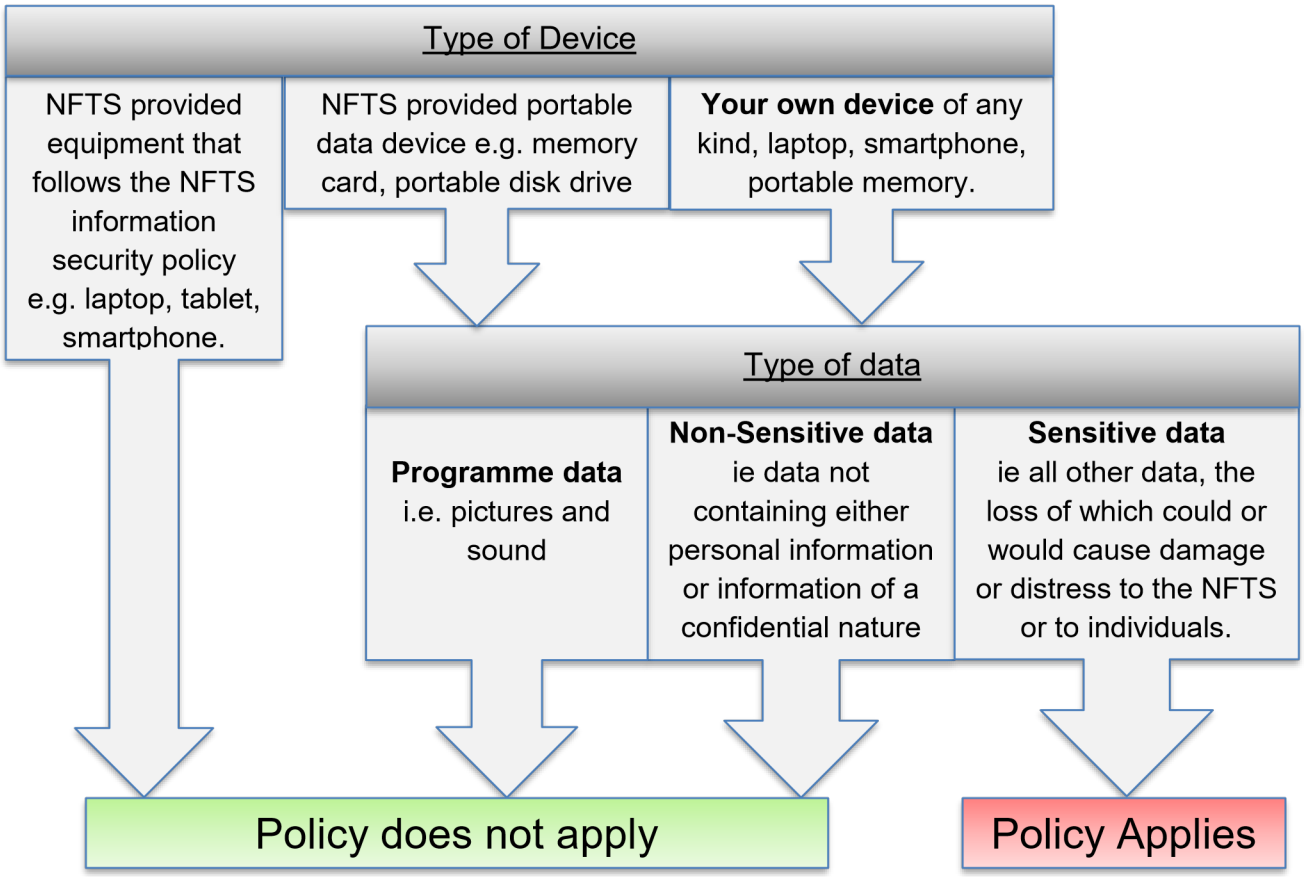
1. Statement of Policy

The National Film and Television School (NFTS) aspires to the highest standards of corporate behaviour, professional competence and best practice in its approach to computing and data security. The School has associated policies relating to Information Security and Data Management. These policies require staff and students and all who have access to, and process, the School's data to keep information secure and to protect personal data. This policy relates specifically to the movement of School data from the School's systems to portable devices and other removable media and the processing of School data on such devices and media. The policy of the School is that information must continue to be kept secure and personal data must continue to be protected when it is transferred on to, or processed on, portable devices and other removable media and during any process of transfer to and from such devices or media.

2. Policy application

2.1. Portable devices are any devices which can easily be carried by hand and be used for mobile computing either in their own right or by being connected to and removed from other computing devices. They include laptop and notebook computers, tablet computers, mobile phones, digital cameras, digital audio devices, portable hard drives, CDs, DVDs, SD cards, memory “sticks” and flash drives.

2.2. This policy does NOT apply to all data – see the chart, below.
If there is doubt about whether data is sensitive of non-sensitive, it must be assumed to be sensitive.



3. Policy Principles

3.1 The dominant principle governing the use of portable devices is:

- Do not transfer the School's sensitive data on to or store such sensitive data on portable devices or removable media unless it is **necessary** for a School business purpose and you have the explicit authority of your Head of Department.
- If it is necessary for sensitive data to be transferred on to or for such data to be stored on portable devices or removable media then the data should be minimised as much as possible, **and**
- The portable device or removable media containing the sensitive data should be an NFTS device and be protected by encryption software in line with the advice and the assistance of the School's IT team to the appropriate current standard.

Data minimisation means minimising the quantity and breadth of data and, where possible, anonymising personal data.

3.2 Staff will ensure that all such devices are protected by a secure password and that the password-protected auto-locking feature (where present) is enabled. Advice on secure passwords can be obtained from the School's IT team.

3.3 The School will abide by legislation and regulations relating to obtaining, using, storing, protecting and disclosing data required in the pursuance of School business.

3.4 The School will provide appropriate organisational and technical measures to help keep data secure and to prevent loss, damage and destruction, assisting staff to implement such measures by producing relevant guidance.

3.5 Individuals processing School data have a responsibility to protect the data from unauthorised use, disclosure, access, loss, corruption, damage or destruction and to adopt all proper and sensible precautions in their handling of sensitive and personal data.

3.6 Any individual using portable devices, removable media or electronic file transfer must ensure that sensitive or personal data are not compromised by inappropriate use of insecure facilities and storage.

3.7 Individuals transferring data on to or storing such data on portable or removable devices shall ensure they have the appropriate authority and approval to do so.

3.8 Sensitive data shall not be processed, opened, read or loaded on public access computers.

3.9 The School's sensitive data will not be transferred to, stored or processed on portable devices or removable media where those data are to be used or accessed by third parties unless such parties have a business relationship with the School and appropriate contractual arrangements are in place.

3.10 Anti-virus precautions should be maintained in all use of removable media devices.

4. Authorisation Process

4.1 For sensitive School data to be transferred on to or stored on a portable device or removable media for use by a member of staff appropriate authorisation shall be obtained from that member of staff's Head of Department.

4.2 The risks associated with transferring data onto a portable device or storing data on it must be assessed and controls to mitigate the risks must be identified and implemented where appropriate.

4.3 The member of staff will complete the appropriate authorisation request and secure the necessary authorisation prior to the data being placed on the portable device or removable media.

4.4 The appropriate authorisation form is available from the IT team

5. Guidelines

5.1 Make sure that you understand what your responsibilities are by consulting the School's Information Security and Data Management policies. If you need further training on data protection matters, get in touch with the School's Head of IT to arrange a session.

5.2 Before using mobile computing devices to process School data, consider whether such processing is necessary. Can it be done without using a mobile device? If it can and the mobile processing is not necessary, then adopt a more appropriate and secure alternative.

5.3 If processing data on a mobile device is necessary, consider whether the data can be minimised, or personal data anonymised, in any way.

5.4 Avoid using removable media devices for permanent or indefinite storage. Make sure data are transferred as soon as possible to a secure, permanent data store and securely removed from all intermediate media. Do not put yourself in a position where sensitive data may be lost irretrievably without a backed-up copy held in a secure School data store.

5.5 Consult your manager to ensure that you have appropriate approval to transfer data on to or to store such data on a mobile device. In order to authorise the transfer of sensitive data on to a mobile device, the Head of Department will need to know that it is necessary and that IT Team guidance has been followed on the appropriate technical measures to keep the data secure.

5.6 If you are a manager, make sure you are aware of any mobile processing carried out by your staff and that the policy is being applied. If you identify that the policy is not being applied despite appropriate briefing and training, then you will need to escalate the matter through your own senior manager, involving HR if necessary.

5.7 Consult the School's IT team (IT@nfts.co.uk) for advice on defensive computing and managing any risks. They will help to identify and implement any appropriate technical measures, including encryption, to ensure the security of the data and/or the device. Specific measures will depend upon the nature of the device.

5.8 Take appropriate physical precautions against the theft or loss of portable devices and removable media. If it is necessary to travel by car with such devices, as well as making sure technical measures such as encryption have been applied, make sure the devices are locked out of sight in the boot of the vehicle. If kept at home, devices still need to be kept secure to protect from opportunistic theft or access.

5.9 If a mobile computing device is disposed of, make sure that the data are properly purged and destroyed. Seek advice from the School's IT Team to ensure that the data are destroyed.

5.10 Software on portable devices and removable media are subject to the same audit procedures as other computer systems. Make sure you have appropriate authority and licence for use.

5.11 Staff should also be aware that portable devices carry a significant risk of inadvertently bringing damaging software or viruses into the School. Following this policy should minimise this risk, but if staff have any concerns that their device may have been compromised, they should report this concern to the IT team (IT@nfts.co.uk)

6. Reporting Data Security Breaches and Lost or Stolen Portable Devices or Removable Media

6.1 All staff should report lost or stolen devices immediately to their line manager and to the School's Head of IT. This will enable an assessment to be made of any loss of data held on the device. Timliness is essential to ensure compliance with data protection legislation including the Data Protection Act 2018 and the GDPR.

6.2 Any security breach of data (or suspected breaches), including those involving portable devices or removable media, should be reported immediately by email to IT@nfts.co.uk.

6.3 A data security breach occurs when there is unauthorised or unlawful processing of sensitive data, including personal data, or there is accidental loss, or destruction of, or damage to such data.

6.4 In reporting the loss or theft of a device and data you are required to identify in writing -
the type of device
- the nature and extent of the data, and
- the security measures which were taken to protect the device and the data

7. Use of electronic file transfers

7.1 The term "electronic file transfer" includes but is not limited to the use of email to send files and data, the use of File Transfer Protocol (FTP) sites to transfer files and data, the use of transfer websites and services such as WeTransfer or Aspera or the use of other organisation's web sites, such as the US Federal Student Aid programme.

7.2 All files that fall under the remit of GDPR must be encrypted before transfer. This encryption can either take place through the website's own system provided the website meets the required standards, or the file must be encrypted before sending. This is particularly the case with email, which in no way can be considered secure. There is no guarantee that transmitted data is received by, and only by, the intended recipient

7.3 Encryption before sending can most easily be accomplished by using a compression programme such as 7-ZIP, as installed on all NFTS systems, and password protecting the resultant .zip file. The password used should meet usual complexity requirements, and should

be passed to the receiving party by a different mechanism to the transfer of the data. At it's simplest this could mean a phone call.

7.4 Data under the remit of GDPR should never be placed in plaintext in an email. Due to the inherently insecure nature of email this could potentially be considered a data breach under the Data Protection Act 2018.

7.5 The use of FTP for any sensitive data is to be discouraged due to the lack of encryption in the transfer mechanism. SFTP or FTPS are to be used instead where data security is required.

Authorisation form for the transfer of data to a portable device or to removable media

This is a request to transfer School sensitive data to and to process those data on a portable device or removable media.

1. Describe the data which are being transferred.

2. Specify why such a transfer is necessary

3. Identify the device or removable media onto which the data are being transferred. Be specific about the name, model and asset number, if any, of the device.

4. Specify the time period for which the transfer will be necessary.

5. Identify the asset owner of the data

I confirm that it is necessary for a School business purpose to make this transfer for the time period specified, that I have the permission of the asset owner to do so and that the data are proportionate to purpose and where possible have been minimized. I will comply with the School portable devices acceptable use policy, including ensuring the encryption of the device or media. I understand that it is my responsibility to assess and mitigate the risks involved and that I will be responsible for the security of the data.

Signed Department

Print Name

Head of Department Authorisation: I authorise the transfer of the data

Signed Department

Print Name

NOTE: A copy of this form, once signed, should be sent to the Head of IT.