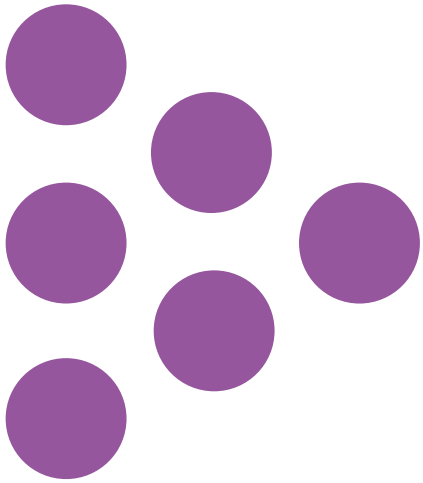
NFER Data Security Policy for NFER Associates

September 2023

National Foundation for Educational Research (NFER)

Restricted



Policy Doc

Version No. V5.0

Next update due August 2024

Contents

This version of the Data Security Policy applies to all temporary workers who support NFER's core business of research and assessment in the UK and overseas, known collectively as Associates.

NFER Data Security Policy

This policy sets out how we will keep information secure to appropriate standards for all aspects of our business. We do this in order to:

- be compliant with the data protection framework set out in UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018)
- maintain and improve our compliance with ISO/IEC 27001, the international standard for information security management systems which will help protect NFER's information
- ensure that we maintain the trust of our customers, research participants, staff and Associates in our work and our ability to manage their data securely and in line with their expectations.

Anyone engaged by NFER must comply with this Policy, and they must also adhere to the Code of Practice and Implementation Guidelines, Data Retention and Deletion Procedures and follow advice and guidance on social media interaction provided by Sales, Marketing and Impact (SMI).

All the policy / procedure documents mentioned in this document are available on the NFER Associates Policy and Training Hub.

This edition of the Data Security Policy is issued as NFER continues the process of moving its IT systems into the cloud. Levels of security will not change but they will be managed differently. As a consequence, some changes have been made to this edition of the Policy, but further updates may be necessary during the year. Associates will be expected to follow and comply with the guidance as it is updated.

1 Aspects of information and data security

This policy covers four aspects of information security:

- the security of our computer systems to protect against unauthorised access
- the physical security of any confidential material which may relate to our work
- the confidentiality requirements we place on our staff and Associates and
- the security of the data that we transfer into and out of our systems.

Underpinning all these is our commitment to data protection. All aspects of our work are conducted in compliance with UK GDPR and the DPA 2018.

By complying with the policy and associated documents, NFER's information assets are protected from all relevant threats, whether internal or external.

It is the objective of NFER that:

- information is made available with minimal disruption to employees, Associates and customers as required by the business process
- the integrity of this information is maintained
- confidentiality of information is preserved
- regulatory, legislative, and other applicable requirements related to information security are met
- appropriate information security objectives are defined and, where practicable, measured
- appropriate business continuity arrangements are in place to counteract interruptions to business activities, and these take account of information security
- appropriate information security education, awareness and training is available to permanent and temporary staff and Associates working on behalf of NFER
- breaches of information security, actual or suspected, are reported and investigated through appropriate processes and learned from when possible
- appropriate access control is maintained, and information is protected against unauthorised access
- continual improvement of the Information Security Management System will be made over time.

1.1 Leadership and the data security group

Information security and data protection compliance is led by an SMT member, Richard Birkett supported by the Compliance Officer, Claire Sargent, and the Data Security Group (DSG). The DSG has representation from all parts of the organisation at a senior level. The group meets formally four times per year, and these meetings are used to review and update policies and procedures, review compliance, discuss risks and to monitor incidents.

The Head of Data Security, assisted by the Compliance Officer, is responsible for the implementation of consistent policies and procedures across the Foundation in relation to compliance with data protection legislation and information security, including the setting up of any associated training and for ensuring that all policies and procedures are rigorous and fit for purpose. The Head of IT Systems Security may deputise for this role as needed. The Head of Data Security, assisted by the Compliance Officer carries out the duties specified for the Data Protection Officer in Article 39 of GDPR.

The Chief Digital Officer is accountable for the security of the IT Network and the provision of the necessary software and data encryption tools to allow NFER staff and Associates to ensure that data in the NFER network is secure. Day to day responsibility for management of the Network is delegated to the Senior Systems Engineer. The Head of IT Systems Security ensures that an

annual penetration test is undertaken and is responsible for any remedial action as a result of the test to ensure that the system remains secure.

The Head of HR is responsible for the security and confidentiality of NFER staff records, including those belonging to Associates. She is also responsible for ensuring that staff and worker contracts of employment support and reinforce the responsibility for confidentiality and data security in relation to their work.

The Facilities Manager is responsible for security at the Slough site, including the physical security of the buildings and grounds, on site visitor management and reception, the CCTV camera network and the secure archiving and disposal of paper materials. She ensures the same levels of security are in place at NFER's other premises.

All individuals carrying out work for NFER on a temporary basis are responsible for ensuring that all the data made available to them for their work at NFER is kept secure. They must comply with this policy, its associated documents and the data protection framework created by UK GDPR and the DPA 2018. See below and section 6 for more details.

2 Data protection

Data protection legislation provides a framework of rights and duties designed to protect personal data (information about an identifiable, living individual). Since the UK left the European Union in January 2021, data protection law is comprised of UK GDPR (a version of the GDPR amended to remove redundant EU references) and the DPA 2018 (similarly updated) as well as Privacy and Electronic Communication (EC Directive) Regulations 2003 (PECR).

NFER ensures that the six data protection principles and the underlying focus on accountability outlined in this legislation are at the heart of its approach to data protection and that individuals' rights over their data can be met. It takes the greatest possible care that the personal data it holds is not unlawfully used or disclosed and that the privacy of data subjects is safeguarded.

Consideration of data protection issues are central to the design of all activities. Data Protection Impact Assessments (DPIAs) are carried out for any new IT system, software / service or application development where personal data is processed. Where NFER's activities process special category data or have particular data protection issues or challenges (such as data sharing between multiple partners), those responsible are required to obtain advice from the Head of Data Security and / or the Compliance Officer on whether a DPIA is required.

NFER and its subsidiary companies pay the data protection fee to the Information Commissioner's Office (ICO) annually. Details are available on the intranet.

Any processing of personal data carried out for NFER by a third party or by NFER for a third party must have a contract which covers all the requirements set out in Article 28 of UK GDPR. Where NFER shares personal data with one or more other data controllers (where there is no contract or other legal agreement between them in place), a data sharing agreement may be required to ensure that all parties have a common understanding of their roles and responsibilities.

Full details of how Associates are expected to ensure that processing meets data protection requirements will be provided as necessary to deployment.

Support, advice, and guidance is available from the Compliance Officer.

Appendix A provides the definitions for key data protection terminology and further information about the six principles.

2.1 Measures to protect personal data

NFER makes sure that it has appropriate technical and organisational measures in place to protect personal data. Some of those measures are to anonymise or pseudonymise personal data which can reduce or eliminate the risks to data subjects.

Anonymisation

Anonymised data has had all identifiable personal pieces of information removed and therefore does not meet the definitions of personal data. If data has been completely anonymised, UK GDPR and the DPA 2018 do not apply to it. However, other aspects of information security continue to be relevant.

For personal data to be anonymised both direct and indirect identifiers must be removed. An individual may be *directly identified* from their name, address, postcode, telephone number, photograph or image, or some other unique personal characteristic. An individual may be *indirectly identifiable* when certain information is linked together with other sources of information, including their school, their postcode or even the fact that they have a particular diagnosis or special educational need. For example, a data file that contained information about a 12-year-old Chinese boy with disabilities in Lincolnshire, could be sufficient to identify that individual.

Pseudonymisation

Pseudonymisation of data means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified. UK GDPR and the DPA 2018 recommends that data is pseudonymised wherever possible when processing special category data or where processing poses high risk.

Pseudonymised data still counts as personal data. Using pseudonymisation techniques helps NFER comply with its data protection obligations and can reduce the risks to the data subjects. It may be one of the appropriate safeguards when processing data for research purposes. NFER teams will consider where it is possible to use pseudonymisation where it is not necessary to retain the direct link between the individual and the data in order to undertake the work.

2.2 Transfer of personal data

The provision of personal data to others can only be undertaken in accordance with the provisions of UK GDPR. Data must only be sent to people or organisations with which we have a contract or formal agreement to provide data and where all aspects of Data Protection legislation have been complied with.

Care should always be taken to check that we have the lawful right to transfer data to the other party. Associates should minimise the amount of personally identifiable data that is transferred out of NFER as far as possible. Data must not be transferred outside of the EEA unless an appropriate safeguard is in place.

3 Information classification

NFER needs to ensure that all data and documents handled as part of its business are kept secure; however, this information has varying levels of sensitivity and therefore requires different levels of protection. Being able to identify the level of sensitivity of our information is key to understanding the level of security that it requires; we therefore classify all information using one of the three levels below. Once the appropriate level of sensitivity is identified, the appropriate control can be implemented to prevent loss, damage, or compromise of the information. It should also prevent disruption of business activities and the compromise or theft of information and information processing facilities. Associates should understand that incorrect classification of information may result in inadequate or incorrect controls being implemented to protect it.

NFER classifies information at one of three levels:

- **Confidential** – containing personally identifiable/special - or high-risk information or confidential materials as designated by contract (for example, confidential tests in development). This information is only to be shared internally with authorised individuals, commensurate with their role or with selected groups. Access is on a need-to-know basis. It should only be shared with Third Parties under strict Non-Disclosure Agreements (NDAs) or contracts.
- **Restricted** – commercially sensitive information which is intended for restricted audiences such as employees or Associates only. It may be accessed by selected NFER employees and Associates, by restricted groups and appropriate third parties under NDAs or other formal agreements.
- **Public** – non-sensitive information which can be freely distributed internally and externally.

All information must be classified (and where practicable, clearly labelled) according to its level of sensitivity (i.e., its classification). Where information of more than one classification is grouped together, the **highest** classification will be applied to all information in the group.

Labelling

All documents produced in the course of NFER's business must carry a classification label. Templates are generally pre-populated. Where an electronic document is being created that has not been tagged with a classification label or does not have its classification pre-populated, the document author must add the classification status to the document, preferably in the footer for printed items and the file name for electronic documents. The classification may be added to a printed document by applying a stamp or writing on it. If a document is only available in a printed format, for example materials to inform and remind staff and Associates of key initiatives, consideration must be given as to where the classification is placed.

The classification status of a document may change over time (e.g., a document may have a Confidential classification early in its life cycle, but this may be downgraded to a Restricted classification as time progresses). Regular reviews of classifications are therefore vital in maintaining appropriate security.

NFER will review and classify as appropriate any information received from outside the organisation when saving it to its network. This may mean replacing the classification mark used elsewhere.

Treatment of information

Confidential

- confidential information should not be sent by e-mail and only be sent using the NFER secure portals or relevant third-party equivalent. Where it is not possible to use portal transfer and by exception only, confidential information may be sent by password protected email attachments. Where password protected attachments are used, passwords must be sent by separate email.

  Note: when OneDrive is released personnel records should be shared using the document share functions of OneDrive. Guidance will be provided prior to its release.
- confidential information should be stored within NFER systems (for example project documents in SharePoint and personnel records in OneDrive). Confidential information should not be put on third-party cloud-based storage systems e.g., Dropbox or Google Drive.
- confidential information should not be verbally discussed in open or public environments; where it is necessary to do so it should only be discussed with staff or contractors with the relevant security clearance.
- storage: physical copies must be held in secure areas and/or locked storage.
- disposal: secure waste bins, shredded.

If working at home, materials classified as confidential should be locked away when not in use and returned to NFER (when possible) for disposal in confidential waste bins.

Examples of confidential information include: personal information (both general and special category personal data), pupil or school staff data, confidential tests, staff appraisals, sickness records, individual salary letters, business continuity plan materials, and pay slips.

Restricted

- restricted information may be shared freely (verbally, electronically by email or fax) with appropriate NFER employees, Associates and contracted third parties.
- restricted information may be stored locally on company issued devices.
- this information is not cleared for release outside the organisation unless there is a relevant contractual agreement in place.
- storage: physical copies do not need to be held in secure areas and / or locked storage
- disposal: secure waste bins, shredded.

If working at home, materials classified as restricted do not need to be locked away but should be returned to NFER (when possible) for disposal in confidential waste bins.

Examples include: contracts, specifications, proposals, project or product documentation, internal strategy documentation, monthly reports, some internal procedures, incident reports, internal telephone directory.

Public

- information which can be released outside the organisation and includes documents or information intended for public disclosure.
- public information may be stored locally on company issued devices
- storage: no restriction.
- disposal: no restriction, recycled.

If working at home, materials classified as public do not need to be locked away and can be disposed of with normal household waste.

Examples include: information widely available in the public domain, public facing website pages, marketing materials, demonstration software, posters and signs used around the NFER offices.

Only information classified as public should be shared on social media – see Sales Marketing and Impact (SMI) for additional advice and guidance.

Clear desks and screens

NFER promotes a clear desk policy aligned to the classification policy above. Associates should not leave information classified as Confidential unattended or on their desks when not in use (neither in the office nor at home). This information should be placed within locked storage when not in use.

Associates should be mindful of the positioning of screens when viewing confidential information, whether working in non-secure areas of the office, at home or in other locations, including while travelling. Applications containing confidential material should be minimised when not in use. All devices should be locked when not in use to prevent unauthorised access to information.

4 Computer systems

4.1 System and equipment security

NFER operates Microsoft Windows Operating Systems and industry standard enterprise software such as databases and email, all managed to recognised industry standards.

Access to the internal network via VPN and other cloud-based services procured by NFER is secured by the use of password and multi-factor authentication. Passwords must be as a minimum a nine-character alphanumeric and contain special characters. They are enforced through the system password policy. A password history of your last 24 passwords is kept and passwords cannot be reused within that period. If there are more than five attempts to access a workstation with an incorrect password, the workstation will be disabled and can only be released by a network administrator or by automatic reset after twenty minutes.

Where possible for cloud-based software applications (for example AdaptiveWork), single sign on using your NFER username and password should be used. If single sign on is unavailable, passwords outside the domain environment should also follow the above password conventions to maintain the security of corporate data. Multifactor verification must be used as the additional step for verifying the user's identity.

Passwords must be kept secure and not shared with others. If access to another individual's account is required, permission must be sought through the individual's Head of department and a written request provided to ICT. Passwords may be shared with IT to allow them to carry out necessary maintenance. Once the necessary work has been completed, the password must be changed.

All NFER laptops and mobile storage devices are encrypted. Associates required to transfer data outside the NFER network must use secure portals or NFER encrypted USB sticks. Only encrypted removable storage devices provided by NFER may be used. A number of these devices will be held by departmental administrators and provided to individuals for their use.

The IT perimeter is secured using firewall technology. These systems are designed to allow or block network traffic entering the internal network. Also based at the perimeter are intrusion prevention systems (used to block vulnerabilities and attacks) and application controls (which allow non authorised software to be blocked).

All files accessed on NFER systems are scanned for viruses including web pages and emails. Email is also protected with anti-spam filters.

All software requires regular updating and patching to minimise the risk of vulnerabilities being exposed. Patches tend to be released regularly and are applied to the servers, laptops, and other computers. IT staff will notify staff and Associates when patches are being pushed out. For some patches to be effective, laptops will need to be restarted. It is the responsibility of the individual to ensure this takes place promptly.

NFER uses UK or European Economic Area (EEA) based data hosting services wherever possible. For certain applications or processes, it may be necessary to host outside the EEA, but this is only by exception. If this is the case, contractual agreements must be complied with in terms of the client's agreement to hosting outside the EEA and appropriate data protection safeguards must be in place with the supplier. Where hosting is needed outside the EEA, the managers responsible must liaise with the Head of Data Security or the Compliance Officer.

4.2 Use of IT equipment

Individuals must lock their workstation (even when working at home) whenever they vacate their desks and unlocking is only possible through entering their own username and password. Services that allow the use of biometric identifiers should only be used when approved by the Data Security Group. Workstations are 'timed out' in five minutes, with the exception of a small number of PCs which are used for specific purposes and have limited access.

All devices must have anti-malware protection (where possible) which is enabled and kept up to date. Users with their own equipment must ensure that such updating is automatically enabled. NFER issued equipment will have the controls installed by the ICT department. Users must not disable or interfere with these controls.

NFER departments and projects have allocated network storage areas. Project areas are only accessible to staff or Associates registered to those projects. Within each drive, project materials and documents are stored within project folders. Storage arrangements will change when we move into the Cloud. Additional advice and guidance will be provided.

Guidance on storage is provided – see section 6.3.

4.3 Use of software

The Head of IT Systems Security must approve all software (free or purchased) before installation or use. The use of cloud-based software is of particular concern as it could be potentially damaging to the organisation if data is not stored within the UK or country deemed to provide an 'adequate' level of protection for personal data.

All suppliers that hold or interact with secure data on NFER's behalf will have a contract requiring them to have suitable technical and organisational measures in place to protect the security of NFER's data. If the supplier processes personal data on NFER's behalf, the contract must cover all UK GDPR contract requirements. The contract must be reviewed and agreed by the Bids and Contracts Team who will discuss with the Compliance Officer or Head of Data Security as required.

Any development of an IT system or application, or significant business change processing personal data will need a Data Privacy Impact Assessment (DPIA). **Work must not start unless the appropriate stage of the DPIA has been signed off.**

When the new system or application has gone live, the DPIA needs to be updated for ongoing developments to ensure that data protection is considered in any future development.

5 Physical security

NFER operates a secure working environment.

The grounds at its Slough site are completely fenced and are monitored by closed-circuit television. All entrances to the building are secured and can only be used by authorised individuals or escorted visitors using a swipe-card system. Associates must use their security pass to gain access to the building. There are various levels of security pass access enabling more limited access to areas where confidential materials or particularly sensitive data are stored. There are extra controls on the use of mobile devices in these areas (see section 6.6.). Security passes are time limited and there are strict controls on changes to the access level of a swipe pass and the issuing of new or replacement passes. All visitors to NFER must sign in at Reception, which is staffed during core hours, and must be escorted around the site. Project offices are positioned so that they are not on the main routes to other parts of the site, so unauthorised visitors are easily detected.

The NFER office in York is located within a secure building and is protected by swipe card or keypad locks. The office is only open when NFER staff are in attendance.

Confidential materials which are paper based, such as test booklets, are locked in cabinets when not being worked on. NFER's courier services provide full movement logging and exception reporting. This must be used when parcels of materials, such as confidential test papers, are to be delivered to and from schools, clients or other individuals or organisations.

6 Confidentiality requirements

Currently, all Associates are required to agree to conditions of service which include requirements to maintain the security of all data. On joining, Associates will be provided with this, the Data Security Policy, and are provided with associated policies and procedures when registering with NFER. All are required to sign and return a statement to HR confirming that they have read them. All are required to re-read and re-sign the confidentiality statement annually or at the point of deployment.

6.1 All Associates

All Associates are responsible for ensuring the security of data available to them in their work at NFER. All aspects of this policy and related procedures and guidance about data protection compliance apply to all staff at NFER, including all permanent and non-permanent staff.

Line managers must ensure that any sensitive information about the individuals they manage is kept and transferred securely.

Associates who use social media to promote NFER and its activities must ensure they follow advice and guidance provided by Sales, Marketing and Impact (SMI).

All departmental managers are responsible for ensuring that the particular requirements for their areas of the business comply with all aspects of policy and procedure in relation to data protection compliance and that the policies and procedures are fit for purpose.

Associates are responsible for managing the relationship with third party suppliers and partners must make sure that they follow the third-party supplier management policy (as set out in the ISMS Management Manual). They must ensure that all necessary due diligence checks have been carried out prior to their initial engagement and where necessary are subject to regular review. There must be a contract or other form of legal agreement for each separate engagement although it may not be necessary to repeat due diligence checks. Contracts with third party suppliers or partners must be approved by the Bids and Contracts team. If the supplier processes personal data on NFER's behalf, the requirements of UK GDPR must be included in the contract. Further information and support are available from the Compliance Officer or Bids and Contracts Team.

Users must follow company practice in the use of portable devices, in particular to keep the devices protected physically from damage, loss, theft or interference so far as is practicable and to report any loss or any potential incident in line with the incident reporting process.

If provided with an NFER device, it should be fully shut down at the end of the working day especially if left unattended in the office or other location. This ensures that highest level of protection (BitLocker encryption, username and password) is in use on the device.

6.2 Training

Associates will be provided with any specific guidance and requirements for each assignment.

Depending on role, this may be a briefing when an individual starts an assignment or attending induction or annual data security training.

6.3 Working outside the office

When Associates are working outside the office, whether at home or in another location (including when travelling for business reasons), they are responsible for the confidentiality and security of all data on which they are working and to which they have access. They should be aware of the higher risks posed to NFER's information by their location and take appropriate care.

When working on restricted or confidential on their personal home equipment, NFER Associates must work within the systems provided by the NFER (for example the virtual desktop, by logging into Office.com with their NFER account or the managed applications provided by Office 365).

See section 7.3. in addition.

No information should be emailed to non NFER accounts other than for legitimate business purposes. This embargo includes Associates' private email accounts.

Associates working at home must not allow other members of their family, household, or visitors to access NFER laptops, virtual desktops, or files.

Working abroad

It is expected that anyone who needs to travel to a third country on NFER business will already understand the data protection and information security implications of that travel on their work. Not all individuals travelling for NFER business will be undertaking the type of sponsored work which has contractual or legislative constraints on where data can be processed; however, if there are any concerns, then they should be discussed with the Compliance Officer prior to travel.

Whilst UK-based Associates can voluntarily request to work overseas temporarily, there are potential issues around the type of data they may need to work on. This should be discussed with the Compliance Officer to make sure that there are no legislative and / or contractual concerns before beginning the period abroad. Contact HR for details of the procedure to following to gain agreement for voluntary overseas working.

6.4 Document and data storage

Associates must work within the systems provided by the NFER (for example the virtual desktop or the managed applications provided by Office 365). Associates must not routinely store any NFER material outside of NFER's network.

All project documents, departmental data and material belonging to cross Foundation groups must be stored in SharePoint (the on-premise version or SharePoint365) or a Networked drive. Note: this includes draft or works in progress. This should mean that there is no reason to store restricted or confidential information (including interview notes that could identify an individual) locally or outside of NFER's network. If circumstances make it necessary for Associates to work on local copies of such documents, they must ensure that the working version is saved to SharePoint at the earliest opportunity and all other versions are deleted.

Where an Associate has an NFER account, the OneDrive associated with that account can be used for personal storage (to hold documentation such as performance reviews and absence forms); it replaces individual's space on the C, J and L drives. OneDrive is cloud-based storage that can only be accessed by you. If required, the account holder can share a file with other individuals for information or collaboration, but they remain in the account holder's OneDrive folder. The account holder retains control over the file and can change or withdraw permission. When you leave NFER and your account is deactivated, material shared in this way will no longer be

available. If you have a personal OneDrive, this should not be used for any NFER business. should not be used for any NFER business.

Note: Guidance on OneDrive will be provided prior to its release.

Although individual departments and teams have their own conventions for file storage, there are some cross-Foundation rules (available on the Information Security and Data Protection pages of the intranet) which must be followed. These will be updated to take into account changes caused by the move of the MS Office suit to the Cloud.

In situations where it will not be possible to comply with the requirement to work within NFER's systems, any working on secure data outside of the NFER's network must be contractually controlled in advance.

Data transfer

Data classified as 'confidential' must always be sent by suitably secure means (see section 3).

NFER will not ask third parties to submit secure data to us by non-secure means.

NFER's data should not be emailed or transferred between staff / Associates to non-NFER devices.

6.5 Sharing information with third parties

Associates must be aware of the classification of material when deciding on the appropriate method of sharing it with a third party. Internally, links should be sent to documents rather than attaching them to an email. When sending confidential material externally, a data portal should be used. IT should be consulted if other methods of data transfer are being considered. Office 365 may give us additional options for sharing restricted and public information with third parties; further information will be provided in due course.

Only NFER issued, encrypted USBs may be used for the transfer of data via portable storage. These are available from departmental admin teams or their equivalent. The data should be removed from the USB when it is no longer needed.

Specific rules apply to the transfer of personal data – see Section 2.2.

Confidential or restricted data must not be posted on or divulged via social media channels; further guidance is available from Sales, Marketing and Impact (SMI).

6.6 Handling materials in the office

Individuals must not search others' desks or work areas to find information about themselves or others, and any such activity may lead to contract termination.

If individuals see that confidential material of any kind has been left in a non-secure location, they should remove the material and lock it away, and make the 'owner' aware as soon as possible. If the owner cannot be identified, please report it to Compliance Officer.

Associate records are kept by both individual managers and staff, and by the HR and Finance teams under secure conditions. When an individual leaves NFER, any files (paper and electronic) held outside HR must be returned to HR.

Mobile phones and other devices may not be used by staff, temporary staff, Associates or visitors in secure areas, with the exception of Microsoft Authenticator. Staff, Associates and visitors should not use mobile phones to capture images of restricted or confidential information. Staff and Associates must ensure that contractors are informed and comply with this rule. Anyone (staff, Associates, contractors or visitors) seen carrying or using a mobile device in a secure area will be asked to put it away.

6.7 Project Director, Project Leader, and Product Manager responsibilities

If Associates are carrying out the role of a project director, product manager or project leader, they are responsible for:

- fully understanding the contractual requirements of their projects or products and ensuring that all project team members understand any particular security or confidentiality requirements that are stipulated by the client, or in law, which require particular actions to take place, such as gaining permission to share data, or seeking consent from participants
- undertaking a risk assessment for all projects and products and documenting outcomes in a risk log using the corporate template. These must be established at the outset of the project / product and updated periodically during the life of the project as appropriate to the scale of the work. Information security risks must be considered in this risk assessment and any risks highlighted on this topic must be provided to the Data Security Group
- completing the UK GDPR Data Log for their projects at start-up and updating the log as changes occur
- ensuring that their projects or products have privacy notices that meet UK GDPR requirements and are actively shared with data subjects before any data processing takes place
- ensuring that the project or product complies with data deletion procedures
- complying with a requirement for completing a DPIA, starting at specification stage and not using systems until sign off for implementation has been achieved
- handling data breach reporting with clients, with approval from the Head of Data Security (as detailed in the breach handling process)
- ensuring that any third-party suppliers or project partners have been approved having gone through appropriate due diligence checks.

6.8 Data deletion and retention

The Data Deletion and Retention Procedures are designed to help NFER to meet legal requirements of the legislative framework for data protection and to provide guidance on how

NFER can protect key documentation that is of value to its business as well as providing a disciplined approach to storage, review and deletion or archive of materials The procedures must be followed by all staff and Associates.

Departmental managers must ensure that Associates are provided with sufficient time and support to follow the Data Retention and Deletion Procedures.

NFER does not currently have a policy which covers the deletion of emails. However, individuals are encouraged to actively manage their in-boxes and follow the principles of the deletion and retention policy.

6.9 Access to the national data sets

NFER's work regularly uses national data sets, for example the National Pupil Database or School Workforce Census, for a variety of purposes. If we are provided with files from a national data set, it will be for a specified purpose and NFER must comply with particular requirements for storage, confidentiality, retention and deletion.

Most access to the National Pupil Database (NPD) is provided through the Office for National Statistics (ONS) Secure Research Service. The Secure Research Service (SRS) is a facility for providing secure access to sensitive data. Only Approved Researchers working on defined and approved projects, which serve the public good, can access this data. Other NFER staff or Associates may be approved to access outputs as part of the publication process. ONS has approved NFER as a safe setting, therefore Approved Researchers can access NPD through NFER's systems.

The SRS operates within a legal framework and there are both personal and corporate penalties for breaking these rules. Anyone who becomes an Approved Researcher to discharge their duties for NFER must read, understand, and confirm their acceptance of the Secure Operating Procedures (SOPs) and the potential penalties. These should be understood for each project using NPD data.

Only ONS Approved Researchers can put in an application for access to NPD and they should email data.SHARING@education.gov.uk to obtain the latest application forms.

6.10 DBS checks (or equivalent)

All NFER staff and workers (both permanent and temporary) undergo pre-employment screening checks including criminal records checks. All Associates working on UK government contracts are required to undergo a criminal record check (unspent convictions only) and to provide a satisfactory Disclosure and Barring Service (DBS) certificate at the level required by their assignment. Associates working in Scotland may require a check by Disclosure Scotland under the Protecting Vulnerable Groups scheme. The level of check required depends on the nature of an individual's deployment and contract requirements. Depending on role and contractual requirements, temporary members of staff and Associates deployed in other areas of NFER's work may also be required to undergo DBS checks at different levels. HR will advise what is necessary.

Full details of these requirements are provided in the NFER Personnel Security Check Policy (available on request).

Permanent members of staff who are required to have an Enhanced DBS check need to update it every two years. This is extended to three years for Associates. Individuals are encouraged to register with the DBS update service to facilitate this requirement. Individuals who work with children, young people, and vulnerable adults as part of their employment fall into this category.

In carrying out its international work, NFER undertakes to apply all reasonable verification checks as part of its recruitment processes.

Associates are required to declare any issues that would be picked up by a criminal records check during the onboarding process and during the course of deployment. Failure to do so could result in the termination of an Assignment and Worker Framework Agreement.

7 Fair usage policy

The Foundation recognises that its website, the internet, e-mail, online communication tools, and telephone systems play a key role in the conduct of its business and that these systems support Associates in carrying out their work efficiently. Nevertheless, the provision of these systems exposes the Foundation to a number of risks and potential liabilities. This section highlights these risks to ensure that Associates understand how they should be avoided.

Communications using NFER equipment or resources should not contain any material which is offensive including (but not limited to) material which is discriminatory (on the grounds of the Equality Act 2010's 'protected characteristics'), illegal, obscene, pornographic, defamatory, harassing, abusive or threatening (including material that has the potential to fall within these descriptions) or any other material that may cause embarrassment to the Foundation, its employees and Associates or its customers.

Failure to observe or conform to this policy, especially relating to the transmission of offensive material (which may be deemed gross misconduct), could result in termination of an Assignment and Worker Framework Agreement.

7.1 Email

E-mail messages emanating from NFER are regarded as official communications from the Foundation. They are classified as 'restricted' (under the information classification policy) and must contain that classification in the email signature.

Emails have the same legal status as written letters and should be drafted with care.

All Associates should ensure that they use the 'blind copy' function when contacting multiple, unrelated external contacts. It is a reportable security breach if this is not done. External members of a project steering committee are considered to be a related group and therefore the carbon copy function may be used. This use of their personal data should be covered in the privacy notice provided for that activity.

Use of a disclaimer (see below) is mandatory when using a Foundation email address. It should be used both internally and externally and must include:

- a full signature which gives the name and position of the Associate
- the name of the NFER, its address and telephone number
- a reference to the NFER's Internet page which gives company information.

Individuals may choose to include their direct line (which can be forwarded to another device when working away from the office) or other number as appropriate.

The approved wording of the disclaimer is as follows:

> National Foundation for Educational Research
> The Mere, Upton Park, Slough, Berkshire SL1 2DQ, UK
> Reg. No 900899 (England and Wales). Reg Address as above.
> Tel +44(0) 1753 574123:
> Web http://www.nfer.ac.uk
>
> This e-mail is restricted to the addressee and may contain privileged information. If you are not the addressee, you are not permitted to use or copy this e-mail or its attachments nor may you disclose the same to any third party. If this has been sent to you in error, please notify us as soon as possible. The NFER reserves the right to intercept and read e-mails sent or received by our employees and Associates. If you do not wish for your communications to be subjected to such scrutiny, you should not communicate via this e-mail system. The Foundation endeavours to exclude viruses from our data but it is the obligation of the recipient to check any attachments for viruses. Opinions, conclusions, and other information contained in this message that do not relate to the official business of the NFER, or are personal to the individual sender, shall not be understood as endorsed by the Foundation and no liability will be accepted. Any legally binding agreement resulting from its content must be made separately in a mutually agreed medium which may only be signed by duly authorised signatories.

Emails and personal data

Sending an email containing personal data to the wrong person (internally or externally) is an information security breach and should be reported to the Head of Data Security and the Compliance Officer.

7.2 Communication tools

NFER's main online communication tool is Microsoft Teams. It provides instant messaging, video, and audio calls. Everyone should consider the appropriateness of their communications when using these tools. Additional M356 applications which will assist with communication and collaboration, such as Forms and OneNote, are also available.

Only NFER approved software should be used to host online meetings with external clients and partners. Associates may attend meetings hosted externally using the host's choice of software.

Teams and Zoom allow users to record online meetings. If the recording function is used for project interviews, the Code of Practice Implementation Guidelines on interview recording should be followed. If a meeting is recorded using Teams, the recording is automatically deleted after 60

days. The meeting organiser will be notified when the recording is to be deleted. Recordings can be downloaded and saved to a project SharePoint site where they must be deleted as part of the project closure process. Any recording made using Zoom should be downloaded to NFER systems and deleted from the Cloud as soon as possible.

Teams (and other software) provide an option to transcribe meetings. Such functions can be used for internal meetings and interviews when it can be used to support accurate recordings of the interactions and outcomes. Transcriptions should be deleted once any minutes or notes of the meeting have been agreed. If these functions are used, all meeting participants should be informed that they are in use and be given the opportunity to object to their use. Details of recording software should be covered in the privacy notice provided for a project or activity.

WhatsApp, the free messaging service, may be used for specified purposes or in extremis when other corporate software (such as Microsoft Teams) is not available. It is used for emergency communication or when normal communication channels are not available. It also provides an easy way for individuals traveling abroad on NFER business to 'check-in' (as set out in the Travel Security Policy). Where Foundation WhatsApp Groups exist, care should be taken to ensure their membership is kept up to date. Any member of a Foundation group should consider the appropriateness of their communication in that Group.

7.3 Using personal devices

Associates may access NFER's cloud hosted managed applications (for example, Outlook, Teams) with their own devices (iPads, iPhones, android phones, and tablets). However, it is a condition of any access to Foundation corporate systems that the individual using the device employs a password protection process to access the device. Should the device be lost or stolen it is the responsibility of the individual to inform the ICT department immediately so they can take appropriate steps to protect NFER data.

Individuals are responsible for ensuring the currency of these applications and making sure that their devices' operating systems are up to date.

If using webmail or other online applications via Office.com Associates should remember to logout when they have finished using them.

7.4 Internet use

Associates must not use NFER equipment to access the internet for the purpose of viewing, downloading, uploading, distributing, storing, editing or recording of material which is offensive, including (but not limited to) material which is discriminatory (on the grounds of the Equality Act 2010's 'protected characteristics'), illegal, obscene pornographic, defamatory, harassing, abusive or threatening (including material that has the potential to fall within these descriptions) or any other material potentially liable to cause embarrassment to the Foundation, its employees or its customers. Such activities may result in the termination of an Assignment and Worker Framework Agreement.

The Foundation employs a number of measures to ensure full compliance with the various legislative and licensing regulations involved with downloading copyright protected web-based

material; individuals are made aware of the need for personal observance of this requirement and their responsibility for adhering to the Foundation's policy.

For either Foundation or personal use, legal requirements must be observed, and copyright ownership must be respected. Copyright applies to all text, digital assets, software, pictures, video, and sound, including those sent by e-mail or found on the Internet. Files containing such copyright protected material may be downloaded but not forwarded or transmitted to third parties without the permission of the author of the material, or an acknowledgement of the original source of the material, as appropriate. For general guidance, one copy of a document may be printed for personal use, but this must not be further copied, unless the website gives permission.

The downloading of any software from the Internet requires approval from the Head of IT Systems Security.

The Foundation will retain the copyright to any material posted on the internet by anyone during the course of his/her duties for NFER.

Any attempts to disable, defeat or circumvent any of the Foundation's computer security facilities may result in the termination of an Assignment and Worker Framework Agreement

7.5 Personal use of NFER provided resources

Where the NFER provides an Associate with resources, the Foundation permits users of its systems to send reasonable amounts of personal e-mail, in their own time and using their personal e-mail accounts (Gmail, Hotmail etc.). Where an individual is making personal use of NFER equipment or resources, they must still adhere to the standards outlined in this Policy; any breach of the Policy will be considered a contractual breach.

The Foundation permits Associates to utilise the internet on NFER provided resources for reasonable personal use. Such use should take place in the individual's own time and not be disruptive to others or their work.

Associates are also permitted to make reasonable and appropriate use of an NFER telephone for necessary personal calls in their own time. They are required to restrict the duration of both outgoing and incoming personal calls. Access to international and premium rate numbers is restricted and permission for access is required from the Head of IT Systems Security.

7.6 Monitoring

Under the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-Keeping Purposes) Regulations 2018, the NFER's Senior Management Team reserves the right to monitor electronic communications made using its equipment or resources for the following purposes:

- recording evidence of business transactions
- making sure Associates comply with Foundation policies
- ascertaining compliance with relevant regulatory practices or procedures

- picking up messages for someone who is absent from work for an extended period (where reasonably practical, this will not be done without the Associate's prior knowledge)
- preventing or detecting crime
- monitoring standards
- preventing computer viruses and maintaining an adequate level of security.

Computers and e-mail accounts are the property of the Foundation and are designed to assist in the performance of Associates' work; individuals should not, therefore, have an expectation of privacy in e-mail sent or received or in the internet sites they access.

The Foundation also carries out random spot checks on its systems which may include accessing any e-mail messages in an individuals' mailbox or checking on specific internet sites they have accessed.

NFER will not normally be looking at personal emails but there may be circumstances when the Foundation requires access to an individual's e-mail or online communication tool account or details of their internet use.

The Foundation may also access an individual's e-mails/monitor their internet use where there are reasonable grounds to suspect that they have misused the Foundation's systems either in the scale, content or nature of messages sent or websites accessed. In these circumstances the Foundation may monitor the destination, source, and content of e-mail to or from a particular address and/or use of the internet from a particular terminal. The Foundation will take the appropriate action where there is evidence of such misuse.

Confidentiality

If for any reason the Foundation requires access to an Associate's e-mail or records of their internet use, any information obtained will be treated in confidence and will not be disclosed to third parties except where, for example, the Foundation is required by law to disclose it.

8 Data breach management

A data security breach can be related to any data loss, threat of loss or any action or activity that could negatively affect NFER's business, brand, reputation, or ability to comply with all data security requirements. A breach includes anything which limits NFER's ability to maintain the confidentiality, integrity or availability of our information and systems. Data breaches are not limited to personal data, they could entail confidential test materials or physical security issues. Where personal data is involved, there may be additional steps to consider.

Full details are provided in the Action Plan for Incident Management.

NFER classifies breaches into three categories:

- **Events** are occurrences that, after analysis, have no or very minor importance for information security.

- **Weaknesses** are usually revealed by repeated breaches that, after analysis, clearly identify vulnerabilities in our system, thereby potentially compromising information security.
- **Incidents** are occurrences that have a significant likelihood of compromising NFER's information security.

Examples of security incidents

Examples of security incidents, which should be reported immediately include (but are not limited to):

- loss of a data storage device containing information (laptops, USBs, hard drives, smart phone etc.)
- failure to maintain the integrity of a dataset
- unplanned downtime of a key information system
- transfer of sensitive or confidential information to an unauthorised external recipient/s
- inappropriate disposal of data storage devices/media
- employees failing to comply with defined security policies/procedures
- employees having inappropriate access to sensitive/confidential information beyond authorisation
- broken door or gate which means that NFER's perimeter is not secure
- exposure of data in a product (for example, Baseline ePortal or NFER Tests Analysis Tool)
- misuse of sensitive information.

Breach reporting

To help us comply with reporting requirements of the ICO, Associates are required to report any breach, threat or potential breach to the Head of Data Security (r.birkett@nfer.ac.uk) and the Compliance Officer (compliance@nfer.ac.uk) as soon as is practicably possible and, at most, within 24 hours of the breach and before any action has been taken. In the absence of the Head of Data Security and Compliance Officer, another member of the Data Security Group must be informed, starting with the Head of IT Systems Security.

The person reporting the breach must also inform the Project Leader and Project Director if the breach relates to a project or inform the Head of Product Strategy and Marketing in the case of a product.

The Head of Data Security will decide who else will be informed, including any external communication requirements. In the case of significant breaches this will include the Business Continuity Lead who will help decide if the crisis management plan should be invoked.

The CEO is informed of all incidents, alerting Trustees as appropriate. In these cases, SMT will also be alerted. If the incident involves evidence of hacking into the NFER computer network or

any other IT related issue, including loss of a laptop for example, the Head of IT Systems Security (or the Senior Systems Engineer in his absence) must be informed.

The Head of Data Security will assess the implications of the breach and identify immediate steps to be taken in consultation with other senior managers as appropriate including implications for:

- clients and NFER staff and Associates, research subjects or other data subjects
- site security
- data loss and hardware recovery
- media contacts and management of external communications and updates
- how to communicate the issue internally and externally.

Information received, decisions taken, and actions authorised will be documented. A simple log will be kept of all categories of breach. Where a significant incident is encountered, this will be recorded on an incident report.

Significant incidents may need to be reported externally to the Charity Commission and / or the Information Commissioner's Office. The Head of Data Security in consultation with SMT and where appropriate NFER's Finance Committee will decide if an incident requires external reporting.

Data protection legislation requires personal data breaches which present a risk to the data subjects' rights and freedoms to be reported within 72 hours. Individuals must cooperate with any requests to assist in any activity related to such an incident as a priority over other activities.

Clients may also report a breach that involves NFER. If this is the case, Associates must immediately inform the Head of Data Security and others (as noted above) of the incident. Any such serious incidents may also need to be reported by the Head of Data Security to the Information Commissioner's Office and, if appropriate, by the Company Secretary via the Finance Committee to the Charity Commission.

Incidents will not be considered closed until:

- all actions have been completed
- any lessons to be learned have been considered and changes arising from them implemented as appropriate
- recipients of leaked personal data have confirmed that it has been securely deleted.

The Head of Data Security is responsible for deciding when all actions concerning the breach are complete.

Appendix A: Data protection principles and key definitions

Personal data:

Data which relate to a living individual who can be identified:

(a) from the data, or

(b) from the data and other information, which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Special category data:

Special category personal data is data about the following:

- revealing racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data, biometric data when used for the process of uniquely identifying a natural person
- data concerning health or data concerning a natural person's sex life or sexual orientation.

In all areas of its work, NFER complies with the six Data Protection Act Principles:

1. **Lawfulness, fairness, and transparency –** data must be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. **Purpose limitation –** we must only collect and process data for specified and explicit purposes and not further process it in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. **Data minimisation –** we must only process data that is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy –** data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data found to be inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.
5. **Storage limitation –** we must keep data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate

technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals;

6. **Integrity and confidentiality (security) –** we must process data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

We are also responsible for complying with and demonstrating this compliance with data protection legislation. This **accountability** (sometimes referred to as the 'seventh data protection principle') takes the form of adopting and implementing data protection policies, taking a data protection by design and default approach, having written contracts with organisations that process personal data on our behalf, documenting the data we hold, carrying out data protection impact assessments, and having an individual (the Head of Data Security) who carries out the tasks of a Data Protection Officer (DPO).

In addition:

- Data must be processed in line with rights of the data subjects
- Data transfer outside EEA is prohibited without appropriate safeguards and individual rights strengthened

Legal basis for processing - All processing of personal or special category data must have a legal basis for processing in place.

Data controller - a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data are, or are to be, processed.

Data processor, in relation to personal data, - any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data subject - an individual who is the subject of personal data.

Data processing - doing anything at all with data – including collection, using, storing, and deleting.

Appendix B: NFER Data Security and Confidentiality Statement

To be signed by all Associates on joining NFER or at the point of deployment

I undertake that I shall comply with all aspects of the NFER Data Security Policy, and any updates issued during the year, in particular:

(a) complying with NFER's document classification systems correctly
(b) recognising and complying with the requirements in my role as described in this policy
(c) reporting all breaches or concerns about data security internally within 24 hours or sooner wherever possible
(d) following any additional departmental or project-based policies or procedures related to handling confidential information
(e) using virtual desktop or VPN or Office 365 applications when working away from the office
(f) following rules for handling confidential test materials, including locking these away when not in use, not talking about the content of this material to anyone not involved in the work, not using mobile phones or cameras in secure operational areas
(g) only using software approved by the Head of IT Systems Security and where necessary reviewed under a DPIA
(h) attending and participating in training for information security and data protection annually if requested
(i) not using any restricted or confidential information other than for my duties as an Associate of NFER
(j) not disclosing any restricted or confidential information to any third party without appropriate prior permission from a Project Director or Head of Department or Centre, both whilst working at NFER or after such time as I cease my employment at NFER
(k) taking good care of any NFER issued devices and using the internet, email and other communication tools appropriately as set out in the fair usage policy
(l) complying with the third-party supplier management policy and only buying goods and services from NFER approved suppliers.

1. I have read the Data Security Policy for NFER Associates and agree that I will work in accordance with its contents. I understand that failure to comply with this policy may will lead to the termination of an Assignment and Worker Framework Agreement
2. Continuing Duty of Confidentiality - I understand and accept that my confidentiality obligations to NFER will continue indefinitely including beyond the termination of my worker framework agreement.

Signed: .....

Name: ..... **Date:** …….