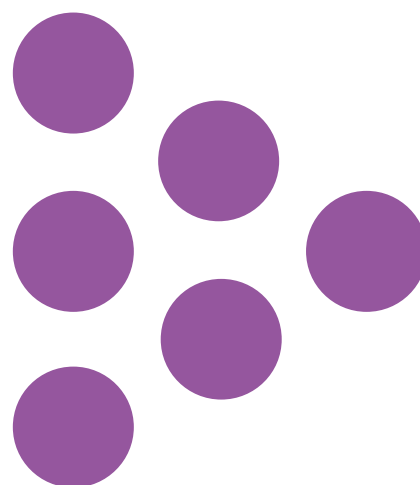# NFER Data Security Policy for Associates

September 2025
National Foundation for Educational Research (NFER)

Restricted

Contents

NFER Data Security Policy

This policy sets out how we will maintain the confidentiality, integrity and availability of the information required to deliver NFER's services (research, assessment and information services for education, training, and children's services) and manage its workforce to appropriate standards for all aspects of our business. We do this in order to:

- be compliant with legal, ethical, contractual, and regulatory requirements especially those relating to 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 assets

- ensure that we maintain the trust of our clients, customers, research participants and 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 , where relevant they must also adhere to the Code of Practice and its Implementation Guidelines, Data Retention and Deletion Procedures and follow advice and guidance on social media interaction provided by SMI.

The Data Security Policy does not form part of your Associate Framework Agreement.

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

As of July 2025, when the employee edition of the Data Security Policy was approved by the Board of Trustees, the information provided in this policy is correct, however, to respond to the constantly evolving threat environment, updates to this policy may be made throughout the year. Associates will be informed of changes and will be expected to comply with the Policy 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

- 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 the UK data protection framework.

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 staff 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, supported by the Compliance Officer, 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

Next update due July 2026

4

All senior staff 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 information security.

All individuals carrying out work for on 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, 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). This legislation will be amended rather than replaced by the Data (Use and Access) Act 2025 which has just received royal assent.

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. Registration 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.

NFER's approach to data protection is set out in a statement on its website. Activity specific privacy notices for our research projects with primary data collections, sale and use of our educational resources and stakeholder communications are available on NFER's website. Privacy information for permanent staff and staff on fixed term contracts is available on NFER Connect. The temporary staff privacy notice is available, on the Policy and Training Hub.

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

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.

The ICO has recently updated its guidance on Anonymisation; the guidance is available on its website - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/about-this-guidance/.

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.

Statistical suppression

Statistical disclosure control is the process whereby we protect the identity of data subjects, and the confidentiality of their data, when using statistical data outputs. Personal data can range from highly identifiable information (and higher risk) such as ethnicity and gender information, to the less identifiable (and less risk), in the form of views and opinions. Any data collected on an individual has the potential to directly, or indirectly, identify that individual.

When considering personal data that has a higher risk of disclosure the minimum count or cell size that should be reported is three, but depending on the level of risk an organization is prepared to take this number can increase. The ONS operate a rule that all outputs produced within the SRS/IDS must have a minimum count of 10. Other organisations use a count of five. Whatever minimum is decided within a project, and this could be different depending on the assessed risk and type of data, a variety of options exist to ensure smaller counts are hidden from disclosure.

For survey outputs, where the data is less likely to be disclosive, small counts of less than three are allowed but the project director must ensure there is no increased risk of disclosure. If there is an increased risk, and this can occur where data is on a specific subject or when it is used in conjunction with other data, i.e. crosstabs, then small counts must be suppressed. The responsibility for ensuring an output is not disclosive rests with the project director.

Suppression options, and other disclosure threats, can be discussed with the Centre of Statistics.

2.2   Transfer of personal data

The provision of personal data to others can only be undertaken in accordance with the provisions of the UK data protection framework. 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. Data should only be shared by secure means.

Care should always be taken to check that we have the lawful right to transfer data to the other party. Consideration should be given to minimise the amount of personally identifiable data that is transferred out of NFER as far as possible. Data must <u>not</u> be transferred outside of the UK unless an appropriate safeguard is in place. Contact the Compliance Officer for advice.

3   Information classification

NFER staff handle lots of data and different types of documents. We need to ensure that it all remains secure. Some of it is more sensitive than others and needs stronger protection. To manage this, we classify all materials at one of three levels depending on its sensitivity. This helps us apply the right level of security and avoid risks like data loss, compromise, or theft of data.

NFER classifies information at one of three levels:

- **Confidential** – containing either general or special category personal data, 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.

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** – commercially sensitive information which is intended for restricted audiences such as internal staff and 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.

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

- **Public** – non-sensitive information which can be freely distributed internally and externally.

  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.

Labelling

All documents produced in the course of NFER's business must carry a classification label. Where information of more than one classification is grouped together, the **highest** classification will be applied to all information in the group.

The classification should be visible to all users. Word templates are generally pre-populated. For electronic documents, the classification may be placed in the file name. 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 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 confidential material

If it is not possible to share a link (with appropriate security settings) to a document, then an NFER secure portal or third party-equivalent must be used. The non-NFER option would be the file

transfer application provided by a client. Confidential information should not be put on third-party cloud-based storage systems e.g. Dropbox or Google Drive. Only when it is not possible to share a link or use a portal for the 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.

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.

Treatment of restricted material

- 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.

Treatment of public material

- 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.

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

Summary table for how each level of classification should be treated

	Confidential	Restricted	Public
Sharing	Need to know basis	Selected individuals only	Freely distributed
Email	May NOT be emailed	May be emailed	May be emailed
Storage of physical materials when not in use (both at home and in the office)	Store in locked storage or secure areas	No need for secure storage	No need for secure storage
Conversations	Avoid discussing in public. Only talk to authorised individuals or contractors.	May be discussed with selected NFER individuals when appropriate	May be freely discussed
Disposal	Confidential waste bin	Confidential waste bin	General recycling

Clear desks and screens

NFER promotes a clear desk policy aligned to the classification policy above. Wherever they are working Associates should not leave information classified as Confidential unattended or on their desks when not in use. Confidential material 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.

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 (as necessary) when patches are being pushed out. For some patches to be effective, NFER laptops will need to be restarted. It is the responsibility of the individual to ensure that patches are installed promptly.

All NFER laptops and mobile storage devices are encrypted.

An IT Health Check, i.e., penetration test, is undertaken at least annually. Ad hoc penetration tests are also undertaken when new systems require them.

Further details of NFER's IT security measures are available in the ISMS technical manual and related IT policies.

4.2   Control of data

To meet legal, regulatory, and contractual requirements, NFER must ensure that it remains in control of its data. NFER has moved more data into the Cloud, which gives staff and Associates improved collaboration capabilities and strengthens resilience, performance, and security. See section 6.4 for details of storage requirements.

Access to data

Access to data is given on a need-to-know basis only. Project and other Teams sites are only accessible to individuals registered to those projects or activities. Project leaders and directors are responsible for ensuring teams are up to date.

Transfer of data

Individuals required to transfer data outside the NFER network must use secure portals.

All USBs are blocked and may not be used for the transfer of data to third parties. In exceptional circumstances, an encrypted USBs may be available from IT.

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 hosting

NFER uses UK based data hosting services wherever possible. For certain applications or processes, it may be necessary to host outside the UK, 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 UK and appropriate data protection safeguards must be in place with the supplier. Where hosting is needed outside the UK, the managers responsible must liaise with the Head of Data Security or the Compliance Officer.

Using your own device

If using a personal laptop, an Associate must use the web-based version of Microsoft Applications (word, excel etc) available at office.com. Using the desktop version of these applications is prohibited. No NFER data should be downloaded to personal devices. For any other personal devices (for example a mobile phone or tablet), Microsoft applications (available from the Apple Store or Google Play) must be used to access NFER owned data.

4.3   Password policy

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 or Erogfy), 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 IT. 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.

4.4   Use of IT equipment

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

It is best practice to shut down and restart a laptop once a day. This ensures that the highest level of protection (BitLocker encryption, username, and password) is in use on the device.

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. 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 IT department. Users must not disable or interfere with these controls.

4.5   Use of software

NFER staff and Associates can only use approved software (both free and purchased).

The acquisition of all software is covered by the Third-Party Supplier Management approval process and starts with the completion of the software request form which can be found on the intranet and must be shared with IT via a Helpdesk ticket.

Once the form is completed, it will be reviewed by IT and may trigger additional processes including the review of the software's security measures. If this process is not followed, it may result in access being blocked.

See the Third-Party Supplier Management Policy (as set out in the ISMS Management Manual) for full details.

As part of the set-up of any new software or application, a Business Impact Assessment (BIA) and associated documentation must be completed by the business and technology owner.

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.

4.6   Artificial intelligence

Generative AI is a new and evolving field which offers many exciting opportunities but also risks. As work to develop a full AI usage policy and guidance is underway the following applies to its use to support work at the Foundation. The following principles apply for any use of AI:

- It must be ethically, legally, and contractually compliant.
- No NFER information can be uploaded to an unapproved AI tool.
- All outputs must be carefully reviewed to check they are robust and accurate.
- All outputs must be labelled as AI generated.

Prior to use both the purpose (the business case) and the security arrangements of the AI tool (whether free or paid for) must be approved. Review of security arrangements is covered by the third-party supplier management process. The business case review will, amongst others, consider tool quality and model transparency, suitability for task, and contractual compliance. Where the AI is intended to support NFER's research activities, the Code of Practice Committee will be involved in the approval process.

In all cases, the first step in requesting approval for the use of AI is to complete the IT software approval form (this includes when an AI element is added to software which has already been approved). A conversation with the IT Business Partnering or Compliance Team is strongly recommended prior to completing a software request form.

Approval for the use of a tool is given for the purpose set out in the business case; any further use must be reviewed separately. Depending on the new purpose, elements of the approval process may not need to be completed again.

Within the Microsoft 365 License provided by NFER, NFER staff and Associates have access to Microsoft's Copilot Chat. Staff can, with care, use this tool to support their work. It is expected that this will be limited to support searching, drafting content generation or summarising. Note, there may be limits on the numbers and types of query that can be asked. As with any other AI output, it must be carefully reviewed to ensure that it is robust and accurate and labelled as AI generated.

Note as the AI usage policy develops the process for approval may change; staff and Associates will be kept informed, and this Policy may be updated.

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 staff or escorted visitors using a swipe-card system. Associates must use a 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 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 Facilities Team manages reception when the office is open.

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

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 Compliance requirements on staff

All Associates are required to agree to conditions of service which include requirements to maintain the security and confidentiality of all data. The requirement to maintain confidentiality continues when an individual has stopped working for NFER.

They must read this Data Security Policy and sign its confidentiality statement on joining and annually thereafter. Records of the signing of the policy are maintained by HR.

Failures to comply with the Data Security Policy may may lead to the termination of an Assignment and Associate Framework Agreement.

The following sections set out other expectations on all staff to ensure that all comply with policies designed to maintain the security of NFER's information assets.

6.1 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. Training on NFERs approach to Data Security is available for you to view on the Associates Policy and Training hub. We strongly recommend that you review this training once you have read and agreed to this policy.

6.2 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 information 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).

Associates should not email any NFER information to their personal email accounts unless it is for legitimate business purposes.

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

Working from public spaces

If for any reason, individuals are unable to work on their own or office Wi-Fi network, it is preferred that they tether to a mobile phone.

If you must connect to a public Wi-Fi, the following should be considered:

- Make sure the device you are using has up-to-date anti-virus and anti-malware software.
- Try to use an encrypted public Wi-Fi network – generally indicated with the word 'secure' and they will probably require you to obtain and use a password. You should avoid the ones that say they are 'open.'
- Switch off the options to 'remember this network' and 'connect automatically.'
- Think about what you are accessing – try to only access less sensitive materials.

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 project and data they may need to work on. Contact the Associates team for details of the procedure to follow to gain agreement for voluntary overseas working.

6.3   Working with third parties

Any Associate 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 also 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.

6.4   Document and data storage

Associates must work within the systems provided by 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. Any exceptions to this are covered in section 4.2 Control of Data.

All project documents, departmental data and material belonging to cross Foundation groups must be stored in SharePoint 365. This includes draft or works in progress. The exception to this would be for statistical analysis and mail merge functionality. In these cases, a networked drive may be used.

If circumstances make it necessary for individuals 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, OneDrive should only be used for personal storage. 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 your deployment ends and your account is deactivated, material shared in this way will no longer be available.

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.

Where services are still on-premises (e.g. Unit4), staff will need to use the Virtual Private Network (VPN) when working remotely to access on premise systems.

Data transfer

Data classified as 'confidential' must always be sent by suitably secure means (see sections 3 and 6.5). It is preferred that you share the document via a link to a SharePoint 365 location, although if this is not possible a password protected document may be used.

NFER staff and Associates should 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. Both internally and externally, it is strongly preferred to send links to documents (with appropriate sharing permissions for the recipient) rather than attaching them to an email. See section 3 for the preferred methods of sharing confidential material. IT should be consulted if other methods of data transfer are being considered.

All USBs are blocked and may not be used for the transfer of data to third parties.

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

Confidential or restricted data must <u>not</u> be posted on or divulged via social media channels; further guidance is available from SMI.

6.6   Handling materials in the office

The classification policy must be followed when dealing with printed materials. Anything classified confidential must not be left unattended.

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 the Compliance Officer.

Associate records are kept by both individual managers and staff, and by the HR and Finance teams under secure conditions.

Mobile phones and other devices may <u>not</u> be used by staff, Associates, temporary staff, or visitors in secure areas, with the exception of Microsoft Authenticator. No-one should 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 seen carrying or using a mobile device in a secure area will be asked to put it away.

6.7   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 staff and 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.

6.8   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 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 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.

6.9   DBS checks

As part of NFER's pre-employment screening 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.

Associates' DBS checks must having issued withing the three years prior to completing an Assignment. Associates who need an Enhanced DBS certificate are encouraged to register with the DBS update service. Individuals who work with children, young people, and vulnerable adults as part of their employment fall into this category.

Individuals are required to declare any issues that would be picked up by this type of check should they arise during the onboarding process and during the course of deployment. Failure to do so could result in the termination of an Assignment and Associate Framework Agreement. In carrying out its international work, NFER undertakes to apply all reasonable verification checks as part of its recruitment processes.

Full details of these requirements are provided in the Pre Engagement Check Policy (available on the Associates Policy and Training Hub).

6.10 Compliance requirement in delivering project work and product development

The table below sets out the responsibility for making sure that all compliance requirements are met when delivering projects and undertaking product development. Although the table focuses on

project delivery, any individual deployed by NFER should apply the principles in the delivery of their work.

	Project director and project leader	**Other members of the project team**
Data protection impact assessment	Responsible	Contribute
Contract or other legal agreement including instructions for personal data processing (when relevant)	Responsible	Contribute
Risk assessment	All team members are expected to be involved in the identification and management of project risks	
	Responsible for identifying and recording risks and regular updating (see project management framework)	Contribute In addition, if designated a risk owner or risk actionee responsible for the mitigation and ongoing update of risks
Maintain project team access	Responsible (maintenance of a SharePoint TeamSite may be delegated)	If project allocations change, highlight requirements for project access to be given or removed as necessary
Complete project data log and privacy notice when relevant	Responsible (task may be delegated)	Contribute to the documents as requested
Follow project closure process with a focus on timely deletion of personal data	Responsible (task may be delegated)	Contribute to the process as requested
Security breaches	Any team member can report an information security breach to the Head of Data Security / Compliance Officer The individual reporting should also escalate within the project team and department	

7   Usage of Communication tools including 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 staff 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 Associate Framework Agreement.

Everyone should remember that there is a permanent record of any written communication transmitted through NFER systems. Even informal exchanges on Teams can be retrieved as part of the response to a subject access request or in dealing with a complaint or grievance. They may function and feel like an informal conversation but when transmitted electronically are retrievable. It is therefore necessary to adopt a professional tone at all times.

7.1   Email

E-mail messages emanating from NFER are regarded as official communications from the Foundation. They have the same legal status as written letters and should be drafted with care. They are classified as 'restricted' (under the information classification policy) and must contain that classification in the email signature (which include a legal disclaimer).

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 name and job title/role

- the name of the NFER, its address and telephone number

- registration details

- a reference to the NFER's website

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.

Blind copy function

Everyone 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.

Potential issues with email

Although a useful tool, emails also provide NFER with a number of potential risks. Everyone should take care not to send email to the wrong people (internally or externally) especially when sharing confidential material or personal data. They should be aware of the restrictions of emailing material classified as confidential; it may not be emailed without appropriate protection (a link is preferred – see sections 3 and 6.5). Sending emails to the wrong address or failing to comply with guidance around emailing confidential material should be reported to the Head of Data Security or the Compliance Officer as they count as information security breaches.

Everyone must also be aware of the risks of **phishing emails**. Failure to identify a phishing email may lead to the compromise of systems. Indicators of a phishing attack could include:

- Poor grammar and punctuation

- Requests from senior staff to action something urgently

- Mismatch between the link you are being asked to click on and the sender's email domain.

Phishing attacks are increasingly sophisticated, and everyone should be on their guard.

Emails sent from NFER staff to Associates will end with @nfer.ac.uk and will generally come from the following addresses:

- associates@nfer.ac.uk

- hrchecks@nfer.ac.uk

- associatepayments@nfer.ac.uk

- TA@nfer.ac.uk

- coding@nfer.ac.uk.

If you have an NFER account and suspect that you have been sent a phishing email you should report it using the 'Report Button' on the ribbon in Outlook immediately or send a screenshot to the helpdesk. Do NOT click on any links or enter any of your credentials (name, email address or password when prompted) or open any attachments. If you are in doubt, it is best to check before doing anything.

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 and other electronic tools.

Only NFER approved software should be used to host online meetings with external clients and partners. Individuals 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. 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 staff and Associates traveling abroad on NFER business to 'check-in' (as set out in the Travel Security Policy). Where Foundation WhatsApp Groups exist, Admins are responsible for ensuring membership is kept up to date, especially when an individual leaves. 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) (see section 4.2 for

further information). 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 IT 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 individuals 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 staff / Associates or its customers. Such activities may result in the termination of an Assignment and Associate 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; please be aware of the need for personal observance of this requirement and your 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 Associate Framework Agreement.

7.5   Personal use of NFER provided resources

Where the NFER provides an Associate with resources, the Foundation permits Associates to use 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 for reasonable personal use. Such use should take place in the member of staff's own time and not be disruptive to other staff or their work.

Where applicable, Associates are also permitted to make reasonable and appropriate use of the telephone for necessary personal calls in their own time.

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 staff 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 member of staff'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 individual's 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 a member of staff'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 individual'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 Breach Management Process.

Examples

Examples of security breaches, 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.)

- errors in a dataset used to contact schools

- 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

- of sensitive information.

- individuals failing to comply with defined security policies/procedures

- individuals 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, the NFER Tests Analysis Tool)

- misuse

Breach reporting

Before any action is taken, a breach, threat or potential breach must be reported to the Head of Data Security and the Compliance Officer (compliance@nfer.ac.uk) as soon as is practicably possible (at most, within 24 hours of the breach). 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. There may also be requirements to inform senior staff in departments.

Prompt reporting helps us to comply with requirements to report data breaches which present a risk to the data subjects' rights and freedoms within 72 hours. Associates 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, individuals must immediately inform the Head of Data Security and others (as noted above) of the incident.

Next steps

The Head of Data Security decides 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 staff 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 process set out in the Serious Incident Reporting Policy will be followed.

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 and annually thereafter

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 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) working within NFER systems (SharePoint 365 or other Office 365 applications, or VPN) as far as practically possible
   (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 (including all forms of AI) which have been through the Third-Party Supplier Management approval process and where necessary reviewed under a DPIA
   (h) attending and participating in training for information security and data protection annually
   (i) not using any restricted or confidential information other than for my duties as an NFER Associate
   (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 with NFER or after such time as I stop being an NFER Associate
   (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 this Data Security Policy for Associates and agree that I will work in accordance with its contents. I understand that failure to comply with this policy may lead to the termination of an Assignment and Associate 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 Assignment and/or my Associate Framework Agreement.

Signed: ....

Name: .... **Date:** ……………