

NFU Policy

Personal Device Data Security Requirements for NFU Officeholders and Secure File Transfer Guide

Written by:
Head of Compliance

Department
Compliance

Valid from:
May 2023

To be reviewed by:
May 2024

The voice of British farming

Although every effort has been made to ensure accuracy, neither the NFU nor the author can accept liability for errors and or omissions. © NFU

N:\current docs\Companies and Compliance\NFU - National Farmers Union\10-Governance\Officeholder_Area\10-Policy_For_Personal Device Data Security Requirements for Officeholders May 2023.docx



NFU SUPPORTED BY
NFU Mutual

1. Purpose

As NFU Officeholders, you are responsible for making sure any NFU information in your possession or control is kept securely and used appropriately. The NFU is committed to ensuring that any data or information shared with NFU Officeholders as part of the fulfilment of their duties is protected, managed and stored in line with data protection legislation and appropriate technical standards.

The NFU understands that NFU Officeholders come from a broad field of businesses and personal situations and hence may have access to and utilise a wide range of IT and security solutions to fulfil their role.

This policy sets out the additional principles, expectations and requirements relating to the use of personal computing devices by NFU Officeholders when those devices are being used to access NFU data, information and resources.

2. Scope

This policy applies to all NFU Officeholders and covers all computing devices whether personally owned, supplied by the NFU or provided by a third party. Use of devices outside of NFU premises is also within scope. Failure to comply this policy will be investigated under the Code of Conduct.

3. Definitions

Cloud services	Systems for storage and sharing of data or hosted software solutions, hosted on third party infrastructure.
Commercially Sensitive Data	Information that, if disclosed could prejudice the NFU's interests.
Corporate data	All files, documents, emails, data in databases and other sources of electronic information belonging to or originating from the NFU. This includes emails, office documents, research and database data, financial data, data obtained from third parties.
Device	Electronic equipment that can be used to access NFU systems or store or process NFU Corporate data. Examples include laptops, smart phones, tablets, USB sticks, disc drives.
NFU Officeholder	Any individual holding a post through election or appointment within the NFU which requires them to access NFU data to fulfil their role.
Organisation	The National Farmers' Union (NFU) or any of its subsidiaries, affiliated companies or entities including but



not limited to NFU Commercial Holdings Limited, NFU Legal Assistance Scheme, NFU Sugar.

Personal Cloud services

Systems for storage and sharing of any data hosted on third party servers set up and managed by individuals.

Personal Data

The Data Protection Act 2018 and the UK General Data Protection Regulations (UK GDPR) define Personal Data as being anything that allows a living person to be directly or indirectly identified.

Sensitive Personal Data

UK GDPR defines Sensitive Personal Data as being in 'Special Categories' of information. These include trade union membership, religious beliefs, political opinions and sexual orientation.

4. Aims

The general aims of this policy are:

- To communicate expectations relating to data security and raise awareness about the importance of information security compliance with NFU Officeholders.
- To protect the NFU and its data subjects from intentional or accidental disclosure of data and illegal or damaging actions.
- To avoid causing the NFU financial and reputational damage.
- To identify requirements with respect to IT Security required to access and utilise NFU information and resources.
- To identify requirements of how NFU information must be electronically stored, protected and maintained.
- To identify requirements on how information must be physically protected.
- To inform NFU representatives how security incidents affecting NFU resource should be reported.

5. Accessing and Utilising NFU information and resources

NFU Officeholders must at all times give due consideration to the risks of using personal devices to access NFU data and in particular, information classified as confidential.

Any Device used to access or store NFU Corporate data must meet the following minimum security requirements listed below:

- Access to NFU Corporate data will be limited to only the individual for whom it is intended.
- Any Device containing NFU corporate data should be physically secured and managed at all times. Devices should not be left unattended in unsecure locations.



- Access to any Device must be protected by strong authentication (e.g. password protection (Biometric, Passcode)). Please refer to the Government Cyber Security service <https://www.ncsc.gov.uk/cyberaware/home> for guidance on creating secure passwords and password management.
- All Devices shall be configured to run commercial anti-virus / anti malware software. This shall be configured to retrieve the latest updates automatically each day, have periodic scanning enabled for all systems and be capable of detecting all known types of malicious software.
- The device must run a current version of its operating system and must also have a recent security update installed. A current version is defined to be one for which security updates continue to be produced and made available to the device.
- All devices, software and system components shall have all vendor recommended system security patches installed to protect the asset from known vulnerabilities.
- Wherever possible all systems and software should have automatic updates enabled for system patches released from their respective vendors. Security patches shall be installed within one month of release from the respective vendor.
- Devices should have the functionality to be remotely wiped if lost or stolen.
- Storage on all devices should be encrypted.
- Any portable or removable storage devices containing NFU Corporate Data must be password and encryption protected. Please refer to the Government Cyber Security service <https://www.ncsc.gov.uk/cyberaware/home> for guidance on creating secure passwords and password management.
- Any Cloud service that may be used to store NFU Corporate data should be done so on a commercial basis with appropriate safeguards in place for management and protection of data.
- Access to Cloud Services that may store NFU Corporate data must be configured with two factor authentication.
- Mobile devices must be encrypted.
- Software firewalls must not be disabled nor updates postponed. Devices capable of employing a software firewall will typically have this enabled by default and set to automatically update.
- All devices must be disposed of securely, including the removal of NFU data before disposal.
- Any use of personal devices by others (family or friends) must be controlled in such a way as to ensure that these others do not have access to NFU data.

In addition to the minimum requirements above, the following recommendations will help further reduce risk:



- Consider configuring the device to “auto-wipe” to protect against brute force password attacks where this facility is available.
- Consider implementing remote lock/erase/locate features where these facilities are available.
- Do not undermine the security of the device (for example by “jail breaking” or “rooting” a smartphone).
- Do not leave mobile devices unattended where there is a significant risk of theft.
- Be aware of your surroundings and protect yourself against “shoulder surfing”.
- Minimise the amount of restricted data stored on the device and do not store any data classified as confidential or above.
- Access restricted information assets via the NFU’s remote access services wherever possible rather than transferring the information directly to a device.
- Be mindful of the risks of using open (unsecured) wireless networks. Consider configuring your device not to connect automatically to unknown networks.
- If a personally owned device needs to be repaired, ensure that the company you use is subject to a contractual agreement which guarantees the secure handling of any data stored on the device.
- Reduce the risk of inadvertently breaching UK Data Protection legislation by ensuring that all personal data pertaining to NFU business, which is subject to the legislation and is stored on the device, is removed before taking the device to a country outside of the European Economic Area.

Transferring data

If an NFU Officeholder is required to send NFU corporate data electronically then this should be carried out securely by using the NFU’s secure file transfer system, not via email or other unsecure methods. Further guidance on sending data securely using file transfer is available in the annex to this policy.

Password Security

Please refer to the UK Government’s National Cyber Security Centre website for guidance relating to email security:
<https://www.ncsc.gov.uk/cyberaware/home>

Destruction of data

On completion of a term of office any NFU Corporate data must be returned to the NFU or destroyed, with confirmation in writing to the Board Secretary or Regional Director. Please refer to the Control of Documents Procedure in the [Governance Handbook Area](#) of NFU Online.



Reporting of incidents and losses

NFU Officeholders have a duty to report the loss, suspected loss or unauthorised disclosure of any NFU information to the Compliance Team (complianceteam@nfu.org.uk). This includes the loss of personal devices, such as phones or hard drives on which NFU information might be held.

You can read more about how to manage incidents involving personal data within the Personal Data Incident Response Plan in the [Governance Handbook Area](#) of NFU Online.

In the event of a breach, involved parties will be required to participate fully with any investigation and remedial action to minimise the impact on the NFU.

Any queries regarding this policy or the use of NFU data should be directed in the first instance to the Board Secretary, Chief Adviser or Regional Director.



Sharing NFU confidential information or personal data.

If you need to share confidential NFU documents or files, email is not a secure method as it is not encrypted and could be intercepted in transit.

There are numerous commercial file transfer solutions available but the NFU provides and recommends you use our data sharing solution.

The following guide explains how to setup an account and utilise this solution which will be available for you throughout your term of office.

The solution allows you to upload files to a secure location on the NFU infrastructure and invite others to access these via a secure link you share via email. The system ensures that any transfer of files is done securely and cannot be intercepted along with additional functionality such as limiting the time a file is available and downloaded.

Requesting Access

To access to the NFU's secure file transfer solution you must first request an account.

To request access please email ITsupport@nfu.org.uk , Requesting access to the NFU file transfer system stating your name and position. You will be emailed confirmation that an account has been set up based on the email address used to request this. Follow the instructions below to access your account.

First Time Login (Once you have received confirmation from NFU IT)

Browse to: <https://datashare.nfuonline.com/>

National Farmers Union Secure File Transfer System



AUTHORISED USE ONLY

Select 'Password Reset' and follow the instructions:

Password Reset

Email

Please enter your email address to reset the password. A confirmation email will be sent to this address.

An email will be sent to the email account entered (this may take a couple of minutes to come through).

N:\current docs\Companies and Compliance\NFU - National Farmers Union\10-Governance\Officeholder_Area\9-Secure_Transfer_Guide_V1_2023.docx

The email will contain the following:

Password Reset Request

Please click on the button below within 1 hour to reset your password:

[Reset Password](#)

This is a Password Reset for the LiquidFiles appliance at: <https://datashare.nfuonline.com>

If you didn't request this password reset, please ignore this email.

If you need assistance accessing or using this system, please contact support at itsupport@nfu.org.uk.

National Farmers Union — Secure File Transfer System: <https://datashare.nfuonline.com>

Click the **Reset Password** button, this will open a web page, enter a password of your choosing following the complexity rules and press 'Save':

Change Password

Password

Password Confirmation

[Save](#)

Password Complexity

Your Password **cannot be based on a dictionary word** and you need at least 3 out of

- At least 8 characters
- At least 11 characters
- At least 15 characters
- At least 1 lower case and 1 upper case character
- At least 1 digit (0-9)
- At least one out of: !, @, #, \$, %, ^, &, *, ? _ ~ - , ()

You will then be prompted to setup Two-Factor Authentication (2FA), this is a secondary method of confirming your identity on top of your password and is current best practise to ensure secure access to systems. You may already use an authentication app on your mobile and this can be used. If you do not already use one we recommend Microsoft Authenticator.

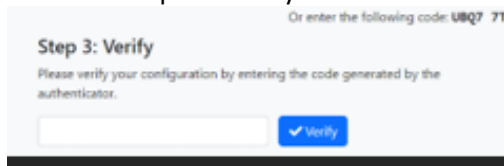
You can download Microsoft authenticator on your mobile by using a link below or by searching for 'Microsoft Authenticator' in your App/Play store:

- [App Store Link](#)
- [Play store Link](#)

On your app select a new account and scan the qr code that is on screen



Once scanned enter the code you are presented in the authenticator app in the verify box in the secure transfer website and press verify:



Logging in

You are now set up to use the system and in future will only need to follow these steps to access the system:

Browse to: <https://datashare.nfuonline.com/>

Enter your email address and password.

National Farmers Union Secure File Transfer System



AUTHORISED USE ONLY

Enter your 6-digit 2FA code from your authenticator app.

Verify Two-Factor Authentication

Please enter the Two-Factor Authentication token from your mobile app.

Skip Two Factor Authentication in this browser for two weeks

Sending a Message

Once logged in, you will be shown a screen to create a message and upload the files you wish to share.

National Farmers Union Secure Messages Support Help

Jordan Oldham (Personal) - oldham.jordan@gmail.com

Message

To: user@example.com

add cc add bcc

Subject: Subject

Message

Tip! Paste content with Control-Shift-V to remove formatting when pasting.

Message Expires: 06/01/2023

Message Expires After: Downloads per Recipient

Send a copy to myself

Private Message

Send

Attached files

Drop Files Here

0 files (0 Bytes)

+ Add Files...

Limitations

Max size: 5 GB (Limited by quota)

[Blocked Extensions](#)

Enter the email address of the people you wish to send files to

Message

To: user@example.com

add cc add bcc

Enter the subject and a brief message

Subject: Subject

Message

Tip! Paste content with Control-Shift-V to remove formatting when pasting.

Drag and drop the files you want to upload or click the **+Add Files** button to add them from a specified folder.

Attached files

Drop Files Here

0 files (0 Bytes)

+ Add Files...

Set how long the link to the files is accessible to the recipients (up to a maximum of a month) and if you want to limit how many times files can be downloaded in the box at the bottom, or leave as the default period.



Then click

Your message will be sent to the recipients and you will receive the following message

Your message has been sent

Message ID	59bPqceE3fCF2QDTSr1RJH
Subject	test
Message Sent	May 18, 2023 15:20
Message Expires	May 25, 2023

Messages Replies

If someone replies to the message you have sent you will receive a copy of that reply in your normal email account so there is no need to log in to the message transfer system to check for these.


View Sent Messages

If you wish to review the messages you've sent you can Click **Secure Messages** top left of the screen and select **Sent** from the options



From this screen you will see any emails you sent, when the files will expire and if they have been downloaded

<u>Recipients</u>	<u>Subject</u>	<u>Filename</u>	<u>Size</u>	<u>Sent</u> *	<u>Expires</u>	<u>Downloads</u>
-------------------	----------------	-----------------	-------------	---------------	----------------	------------------

Select the  at the right of the message to do one of the following:

- Delete the attachments
- View the original email sent