Managed File Transfer

Managed File Transfer (MFT) allows Ofcom to share files with external organisations securely. It provides a full audit trail of activity. There are two methods for sending and receiving files – shared folders and Packages. Your Ofcom contact will arrange the most appropriate one for your purposes.

Packages

For one-off file transfers or occasional use, MFT provides a secure Package facility that works in a similar way to email messaging.

You do not need an account on MFT to access a Package. When someone from Ofcom sends you a package you will receive an email notification from MFT with a link to the Package.

Your Ofcom contact will provide you with a password to access the package. You can then download any attached files.

To send data using this method, someone at Ofcom must first send you a package. You can then reply - attaching any files you want to share with your Ofcom contact.

Shared Folders

For users who need to transfer files to or from Ofcom regularly, MFT provides a secure transit folder facility. Your Ofcom contact will request an MFT account for you. They will be asked to provide your name, email address and company name.

A unique username will be created for you.

Once your account has been created, your Ofcom contact will notify you of your temporary password separately. You will be required to change this when you first log on to MFT.

After logging on you will be able to navigate to the shared folder to upload or download files as agreed with your Ofcom contact.

Security Fact Sheet

- During transport MFT uses TLS to encrypt communications. The minimum strength of the encryption used during web transport is 128-bit and the system is regularly penetration tested.

- MFT stores all files on disk using FIPS 140-2 validated 256-bit AES. Each file has a unique encryption key, which is also encrypted.

- MFT logs all sign-on and sign-off events, permission changes, new user additions and other actions which directly affect the security of the system. All log entries are cryptographically chained together in a way that makes any tampering of audit logs evident.

- MFT uses cryptographic methods to verify files have not been tampered with.

- Please note that MFT is a tool for transferring files only. To prevent data falling fallow, files are automatically deleted after a set period.

- Only encrypted Zip file format (.7z or .zip) files should be uploaded into MFT.