Recommended data storage at JU for staff

	Normal data	Sensitive data
Personal data	• Onedrive	• Personal JU Files
Shared data	• Common Staff Public • Office365 Teams	• Common Staff Restricted • JU Sharefiles

For specific cases, we also recommend data storage at NAS or with collaborating companies.

Onedrive

Suitable for: Personal data not classified as sensitive
Stored on: Encrypted cloud storage hosted by Microsoft
Account: JU account
External access: Via the internet
Storage space: 1 TB
Backup: Version management and short-term backup readback

Common Staff Public

Suitable for: Shared data at a company or department level where the data is not classified as sensitive
Stored on: Local encrypted storage at JU
Accountd: JU account
External access: Via VPN connection to JU's network
Storage space: 50 GB, can be increased if needed
Backup: Backup with two month readback capacity

Office365 Teams

Suitable for: Shared data for a group of users where the data is not classified as sensitive
Stored on: Encrypted cloud storage hosted by Microsoft
Account: JU account and invited guests
External access: Via the internet
Storage space: 1 TB
Backup: Short-term backup readback

Personal JU Files

Suitable for: Personal data classified as sensitive
Stored on: Local encrypted storage at JU
Account   JU account
External access: Via VPN connection to JU's network
Storage space: 50 GB, can be increased if needed
Backup: Backup with two month readback capacity

Common Staff Restricted

Suitable for: Shared data for a group of users where the data is classified as sensitive
Stored on: Local encrypted storage at JU
Account: JU account
External access: Via VPN connection to JU's network
Storage space: 50 GB, can be increased if needed
Backup: Backup with two months' readback capacity

JU Sharefiles

Suitable for: Shared data for a research project with external users where the data is not classified as sensitive
Stored on: Local encrypted storage at JU with access control for folders and delegated administration
Account: JU account and invited guests
External access: Via the internet
Storage space: 50 GB and 10 users, can be increased at a cost
Backup: Version management and backup with two month readback capacity

Specific needs:

NAS: Local storage at JU of large volumes of data with lower performance and lower operational security
Company: If specific security requirements apply, it is recommended that the data is stored by the company which has these requirements.

Sensitive data

Information subject to secrecy provisions of the Public Access to Information and Secrecy Act or breaches of the law and sensitive personal data subject to the provisions of the General Data Protection Regulation

Confidential cases (example)
Confidential data for staff and students
Health conditions, transfers, secret addresses, discipline cases
Confidentiality to protect economic interests
Business and operating conditions, offers/procurement
Confidentiality within research
Commissions, patents, collaboration, statistics, transfers

Sensitive personal data (example)
Sensitive personal data that reveal ethnicity or origin, political opinions, religious or philosophical convictions, trade union membership or personal data concerning health or sexual preferences. Health data may relate to sickness absence, pregnancy or medical appointments.

Law violations (example)
Personal data on law violations, which include offences, criminal convictions, coercive measures or administrative deprivation of liberty.

If you need advice and support when it comes to information safety, confidential data or the processing of personal data, please contact the HS Planning Department