Security of data and information

There are a number of options available to staff and students when deciding what to use for file storage or file transfer. Some of these options will be limited based on circumstance and the classification of information you are dealing with:

The video below shows some of the security services that are in use at Lancaster to protect the information you and the University.

Based on information classifications, you can ascertain what level of protection is required when storing information for the purpose of Information Security.

There are a number of methods available for you to use – the choice of the storage method would depend on the information classification and circumstances (e.g. whether it is paper based information, whether your department has any extra rules/regulations that you need to consider etc.)

The table below summarises some possible storage methods, depending on information classification. There is further information about what cloud services are/are not permitted to use for University data on Storing information in the cloud.

### Mobile / External storage device
- Ordinary: Acceptable
- Confidential: Encryption recommended
- Restricted: Encryption required (FIPS 140-2 compliant)

### Personal / Research /Departmental filestore
- Ordinary: Acceptable
- Confidential: Acceptable, with restricted access

### University Microsoft Office 365 services (e.g. OneDrive, Teams, SharePoint)
- Ordinary: Acceptable**, including special category personal data (sensitive personal)
- Confidential: Encryption required

### Other cloud storage
- Ordinary: Acceptable
- Confidential: Encryption required
- Restricted: Encryption required
- Personal data NOT permitted in other cloud providers

### Paper based documents
- Ordinary: Unlocked storage
- Confidential: Locked storage recommended
- Restricted: Locked storage required

**When sharing personal data externally a data sharing agreement or contract with GDPR clauses should typically be in place (unless we have consent of the individuals). These should be in place for any data sharing arrangements that are already set up, but you are advised to check it is the case. For any new arrangements, the Information Governance Team can be contacted for advice.

Based on information classification, you can ascertain what level of protection is required when sharing or transferring information for the purpose of Information Security.

There are a number of methods available for you to use – the choice of the transfer method would depend on the information classification and circumstances (e.g. whether it is paper based information, whether you want to transfer information between departments on campus (internally), whether your department has any extra rules/regulations that you need to consider, etc.)

The table below summarises some possible transfer methods, depending on information classification.

<table>
<thead>
<tr>
<th>Electronic information</th>
<th>Paper based information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sending externally</td>
<td>Sending internally</td>
</tr>
<tr>
<td>Ordinary</td>
<td>Confidential</td>
</tr>
<tr>
<td>----------</td>
<td>--------------</td>
</tr>
<tr>
<td>- Teams</td>
<td>- Teams</td>
</tr>
<tr>
<td>- OneDrive</td>
<td>- OneDrive</td>
</tr>
<tr>
<td>- Email</td>
<td>- Email</td>
</tr>
</tbody>
</table>

- Teams with appropriate team membership
- OneDrive
- Email (encryption required)
- Shared folders (departmental / research)
- SharePoint site with appropriate access permissions

- Teams
- OneDrive
- Email
- Shared folders (departmental / research)
- SharePoint site with appropriate access permissions

- Teams with appropriate team membership
- OneDrive
- Email not recommended, if no other alternative, must encrypt
- Shared folders (departmental / research)
- SharePoint site with appropriate access permissions

- Recorded / Special / Courier delivery
- Sealed envelope in internal mail (ideally hand deliver)
| Personal data | Teams with appropriate team membership/via chat  
|              | OneDrive  
|              | Is it possible to remove information (e.g. a name) and send non personally identifiable information (e.g. ID number)  
|              | Email not recommended, if no other alternative, must encrypt personal information before emailing  
|              | Departments/research  
|              | SharePoint site with appropriate access permissions  
|              | Is it possible to remove information (e.g. a name) and send non personally identifiable information (e.g. ID number)  
|              | Email not recommended, if no other alternative:  
|              | Encryption required if contains personal information of more than one person*  
|              | Encryption recommended if it’s about an individual and sent internally*  

* Depending on the content of the information you are transferring, you need to apply a sensible /realistic level of protection (be pragmatic).

---

Once you no longer need information, you will want to dispose of it. Lancaster University data retention information is available online. Please dispose of information appropriately – whether it's electronic or paper based information.

No media should be released for disposal if it contains restricted, personal or unclassified information (and therefore may contain restricted or personal information). It must be disposed of appropriately.

It is important to remember that simply deleting and reformatting will not remove all traces of the information as some specialist software can access files that look like they are no longer there.
To dispose of media with restricted, personal or unclassified information:

- Use a computer disposal company that offers secure media disposal (if it is an electronic device, please make a disposal request via this form).
- Printed materials – Please ensure restricted or personal information is shredded or placed in confidential waste. Confidential waste bags are available from your department. Ordinary information can be disposed of in a waste recycling bin.