Information Security

Information Sharing Policy

Version 1.1:
Approved March 2019
Review June 2023

Information Sharing Policy

1. Policy Overview

The work of the University requires the sharing of information between staff, between staff and students, and between staff and (external) third parties. Seeking to maintain the open nature of the organisation, whilst also minimise the risk of loss, unauthorised disclosure, modification or removal of information maintained by the University; this policy section aims to provide members of the university clarity on sharing information in a safe and secure manner. This policy covers information categorised as Confidential under the University's Information Categories and Controls Policy.
A3dners inf5 (w)135pltraty on s.5 fp(c)-2 (l)2.6o(or)-6 (i (he)10..6 (and)10.5 (()66 (ex)8.9 (t)-67

4. General Guidance

Staff should be mindful to ensure they are handling information and applying appropriate safeguards in accordance with the Information Categories and Controls Policy.

Draft documents should normally be considered as ‘Confidential’ until they have been finalised or approved through the relevant line management or governance arrangements.

A flow sheet has been developed to help individuals make informed decisions when considering the sharing of information, t is the responsibility of those releasing the information to ensure that the recipient understands the confidentiality of the information and will abide by the provisions of this policy.

The remainder of this policy relates to the sharing of Confidential information.

5. Data Owner

thishosu4.96hathio-2 (t)-6.6 (he)104.9 (m)-e2 (ha)14.4(m)-be.4n6es 6fye tthos0.5 (r)-2 (ha)10.5

to specific projects. However, it must be sought on a case by case basis when any unusual or non-standard use is to be made of University information. If ownership is not clear, this should be referred to the Information Governance Sub-Committee for guidance.

6. Sharing in Hardcopy Format

Sharing of Confidential Information in hardcopy form is discouraged as further sharing by the recipient remains easy and there is considerable risk of this information not being maintained or disposed of securely. If such sharing is undertaken, checks should be made on the arrangements for appropriate storage and disposal, and these should comply with the relevant University policies. For example, policy on the Management of User Access Information, and the University Records Retention Schedule.

7. Sharing in Electronic Format

beit foriieic R iaon n.6 (i)-6.7 (o)11.2 (r)e5 >>BDC /-3.9 he toi
Information is most frequently shared in electronic format. Such formats make information easy for recipients to share, potentially when it is not appropriate to doat ap.1.141 TD

If it is essential to send confidential information via an email, or email attachment, to email addresses outside of the University, the potential risks to the security of the data should be considered and where proportionate a Data Privacy Impact Assessment (DPIA)

If saving and sharing information via one of the above media is considered to be essential as it is deemed to offer significant advantages over use of one of the previously recommended, more secure approaches, the user must ensure:

- That anti-virus software is present and up to date on machines which data is taken from and machines which data is transferred to;
- All data is held on encrypted mobile/removable storage and devices at all times.

Information on anti-virus software and encryption of information can be found at:

- Staff: anti-virus
- Student: anti-virus
- IT Operations: Encryption Policy

Users wishing to transport and/or share Confidential information using electronic media MUST also ensure:

- The data on the device is encrypted to the highest recommended encryption standard (AES-256). Please contact IT Services for further assistance;
- Compliance with any certified level of encryption required under a research or other grant or contract (e.g. to a standard such as FIPS-140-2). If such requirements are stipulated, please contact IT Services for further assistance;
- Mobile devices and/or electronic storage devices containing Confidential information should not be sent off site without the prior agreement of the data owner. IT Services should be consulted to ensure the level of security is appropriate for the type of data being transferred;
- Electronic media used to store Confidential information shall only be used by authorised individuals and where there is a clear business need;
- Data stored on the electronic mediasc2kI]TJxb 0 Tt2 x k be I T

beiow 2.272 s/TT0 1 Tf 0.4ow 2

.0.016 0 0.272 Tw Td [00.002 sc0 tat2<0078>Tj. Td ( )Tj -0.0019 88

Document Control

Version	Author	Date	Version Detail

V0.21	Claire Vallance, Gareth Cole, Mark Lister, and Matt Cook	29th January 2019	To include more clearly defined references to Research and Ethics processes. Policy to incorporate risk, authorisation, and possible enforcement.
V0.22	C Tw 9.960 0 9.96 2(,)-1.1 (		