Information Sharing & Transfer Policy

Version	1.1
Reviewed Date	22/05/2023

1 Introduction

1.1 The University holds a large amount of information, both in hard and soft copy. This includes personal and special category data (as defined by the UK Data Protection Act, 2018), and also non-personal information, which could be sensitive or commercially confidential (e.g. financial data).

1.2 Sometimes it is necessary to share personal data or information when we are working with partner organisations or other institutions or on collaborative projects.

This might entail:

- The University may receive personal information from the institution or partner
- The University may send personal information to the institution or partner
- A request for personal information held by one or more parties

1.3 These partners might be our partner colleges or universities, or other institutions with whom we have a relationship. We may or may not have a formal contract with these institutions or partners. Therefore we must consider what legal requirements there are associated with sharing information in the context of privacy and confidentiality.

2 . Information Sharing

2.1 Disclosures of information (sharing) should be relevant, proportionate and lawful.

2.2 All regular sharing of information to the same source should be governed by a data sharing agreement which sets out the protocols for:

- What data is to be shared
- For what purpose
- Legal justifications for sharing
- Benefits and risks of sharing
- Information lifecycle (retention and disposal)
- Responsibilities and liabilities in the event of information security incidents
- Agreed methods of transfer
- Appropriate audit trails and governance

- Appropriate ID and background checks (where applicable)
- Identifying points of contact in the event of a security incident

3 Methods of Transfer

3.1 Electronic Documents

3.1.1 Sufficiently secure methods must be used when transferring personal data.

3.1.2 In the case of confidential and/or sensitive data it is recommended that data is encrypted to an acceptable standard (i.e. compliant with FIPS 140-3) prior to transfer and protectively marked.

3.1.3 Encryption passwords must not be relayed using the same communication channel as the data.

3.1.4 An audit trail of all transfers must be maintained in line with the retention policy.

3.1.5 If transfer is by email, information must be sent to named persons where possible, the use of group mailboxes is to be avoided.

3.1.6 Information no longer in use by either party must be securely deleted.

3.2 Hardcopy Documents

3.2.1 All hardcopy data must be posted using the University's approved mail delivery company.

3.2.2 All confidential and/or sensitive data must be identified and sent with the appropriate level of tracking via the University's approved mail delivery company.

3.2.3 Personal information must be labelled '*private and confidential' and 'addressee only* where appropriate.