Policy: **ISP-I12**
Title: **Allowing off-site access to the Shared Departmental X: drive – Guidance Note**
Status: **Approved**

1. Introduction

1.1 The University's default position is that off-site access to a departmental x: drive is not permitted except where approval to do so has been given by the Head of Department or Head of Division. The concern is that offsite access to the X: drive significantly increases the risk of unauthorised access to information in the event of security being compromised.

2. Risks

2.1 A University IT account username and password is required to access the Shared Departmental X: drive both on and, where permitted, off-campus. Should a third party obtain the password of a staff member this would give them access not only to the staff member's own account information, including files and emails, but also to departmental information held on the X: drive to which the member of staff has been granted access.

2.2 A password can be compromised in a number of ways including:

a) Phishing emails luring staff members into revealing login information.

b) Shoulder surfing, i.e. people observing (and even videoing) staff members logging into devices and taking note of their username and password.

c) Key logging devices attached to personal computers which record login details.

d) Viruses on devices, which similarly record login details and then transmit to hackers.

e) Compromised wifi hotspots, which monitor and record activity.

2.3 This is an existing concern, however if offsite access is granted to the X: drive the degree of exposure is increased significantly. Currently a third party in possession of login information would need to be physically on campus in order to access the X: drive. If offsite access is granted to a department, this will no longer be the case. A third party would not have to be on campus. The departmental X: drive would be accessible from anywhere in the world.

2.4 It should be noted that, in the event of a breach of personal data, depending on the numbers of individuals or the sensitivity of the information concerned, it may need to be reported to the Information Commissioner. The Information Commissioner in such cases will assess whether appropriate measures were in place to protect the information based on its sensitivity and could take enforcement action and/or levy a fine of up to £500,000. In either event, there would be significant reputational damage.

3. Reaching a Decision

3.1 Notwithstanding the above, it is anticipated that most departments will request remote access. However, for some departments they may consider that the exposure is unacceptable or contravenes contractual obligations, and decide that offsite access to the X: drive is inappropriate.

3.2 In deciding whether or not to request offsite access for the X: drive there are a number of factors that should be considered including:

a) Does the X: drive contain the personal data of staff, students or other individuals? This would include information such as name, gender, address etc.

b) Does the X: drive contain the sensitive personal data of staff, students or other individuals? This would include information relating to mental or physical health, ethnicity, sexuality, trade union membership, criminal convictions etc.

c) Does the X:drive contain confidential or sensitive information that may be considered the intellectual property of the University or others, or research data, that could affect the interests of the University or other organisations if security were breached.

d) Does the X: drive contain any other information that may be of a confidential or sensitive nature that could affect the interests of the University or other organisations, if security were breached?

e) Are there contractual obligations on the security of information in relation to third party commercial and/or research partners?

f) For information of a highly confidential nature (e.g. sickness, appraisal, disciplinary records) is access restricted, as far as it is practicable, to only those staff who have need to access the information?

g) How large is the department? What number of people would potentially be able to access the X: drive externally?

h) Have all staff completed the Information Security Awareness training course?

i) Are staff aware of the implications of their password being compromised?

3.3 Most of the above checks will need to be done in consultation with other staff within the department. Confirmation of whether staff have completed the Information Security Awareness training course may be obtained from Information Assurance Services (email ias@le.ac.uk, tel. 0116 229 7946).

3.4 The decision whether to allow off-site access to the X:drive must be made by the Head of Department or Head of Division who has responsibility for the security of data within their area.

4. Matters for consideration after a decision is made

4.1 Once a decision has been made, there are still matters that should be considered. A list of recommendations is included below. These are important considerations irrespective of whether the decision is yes or no:

a) All staff within the department must complete the online Information Security training.

b) Regularly reiterate the importance of strong password management to staff and ensure that if they feel there is even a chance their password has been compromised that they should take measures to change it.

c) To the extent that it is practicable, ensure that access to each folder containing information of a personal, sensitive or confidential nature is restricted to only those staff which require access to the information.

d) Do not allow more open access to folders containing information of a personal, sensitive or confidential nature simply for administrative convenience.

e) Where offsite access is permitted, although all staff within the department would be able to access the X: drive externally, thought should be given to identifying staff who should be discouraged from doing so because it is unnecessary.

f) If there is a need for offsite access to the X: drive but there is also certain information for which this is not acceptable/permitted, please consult with IT Services and Information Assurance Services to see how this may be addressed. Under no circumstances should unofficial workarounds, such as the use of external hard drives or the C: drives, be used.

g) Ensure all contractual obligations regarding the security of information are being met.

h) With the exception of postgraduate research students, students should not be granted access to the X: drive. Where there is a need to provide students with access to file stores this should be done using the T: drive or Blackboard.

i) If it is decided not to make the X: drive accessible offsite, measures should be taken to ensure that staff do not resort to alternative means of gaining access to files offsite which are fundamentally less secure. e.g. use of Dropbox, emailing of files, use of an unencrypted USB memory stick.

Failure to comply with University Policy may lead to disciplinary action.

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.