Preamble

1. The University’s Audit & Risk Committee (ARC) has issued a directive which requires University-owned laptop PCs to be encrypted, in order to reduce the risk of an unauthorised disclosure of sensitive information, due to accidental loss or theft.

2. Properly encrypted laptops will protect personal information (as defined by the Data Protection Act), as well as securing research information, University financial and business information and confidential internal documents.1

3. Encryption protects the University’s assets against loss or theft. It does not alter the need for laptops to be otherwise operated and managed securely (to prevent other forms of data loss), for example by being properly patched, and ensuring that any valuable information is securely backed-up.

Scope

4. All laptops purchased with University funds are owned by the University, and this policy applies to them.

5. All laptops will have a named “custodian” (nominally the person who requests the purchase of the laptop), who is responsible to the University for any laptop(s) in their charge. This information will be recorded in the University’s Asset Register.

6. It is the responsibility of individual members of staff to ensure that they comply with this policy, and to ensure that all laptops of which they are custodians comply with this policy.

7. If any laptop is not capable of supporting the operation of encryption software (e.g. the machine is of very low specification and/or is too old), it will need to have all sensitive information removed (in order to ensure it no longer breaches the University security policy). Where it is necessary to continue to process such information, a new laptop, capable of supporting encryption, must be obtained.

Policy

8. All University owned laptops will be encrypted by means of the University’s managed encryption service.

9. All laptops supplied by the University will have University’s managed encryption software enabled by default.

10. In a limited number of circumstances, it may be appropriate to exempt a laptop from encryption; details of the exemption process are described below.

11. The Service Centre, or School IT staff, where applicable, will be able to advise on and arrange for laptops to be encrypted.

1 Collectively, these will be referred to in this document as “sensitive information”.


Exceptions

12. There may be a limited number of cases where it may be necessary to operate a laptop without encryption. Details of the exemption process may be found in Appendix A. In summary:

- **No** exemption to encryption will be permissible where personal data (as defined by the DPA) is involved.
- A written exemption, duly authorised by either the University’s CIO, the Chief Technology Officer (CTO) or the Information Compliance Officer (ICO) is required for each laptop, and must be renewed annually.
- The University’s CIO, CTO or ICO may authorise an **audit of any laptop, at any time**, to verify compliance with the terms of the exemption.

Non-compliance

13. *The University’s CIO, CTO or ICO may authorise the inspection of any University laptop at any time to establish compliance with this policy.*

14. Where any member of IT Support Staff becomes aware of the operation or use of an unencrypted laptop without an authorised exemption (see below), they will record this fact, and report it to the University’s Chief Information Officer, Chief Technology Officer or Information Compliance Officer for further investigation.

15. Information in respect of non-compliance will be routine reported to the University’s Audit & Risk Committee at as detailed a level as is deemed appropriate. ARC will determine what sanctions, if any, are appropriate.

Reporting

16. The loss of any laptop belonging to the University must be reported to the Response Centre and to IT Service Desk (www.city.ac.uk/itservicedesk)

17. The use of a University laptop without either encryption or a valid exemption should be reported to IT Service Desk (www.city.ac.uk/itservicedesk)
Appendix A: Exception Policy

There may be a limited number of circumstances in which a laptop custodian wishes to use an unencrypted laptop. This procedure describes under what circumstances such an exemption may be obtained.

1. An exemption may be authorised where no sensitive information is held, where only trivial amounts are held, or where such information is only held transiently.

2. The device does not meet the minimum standards necessary to run the University’s managed encryption software. In such circumstances, either:
   i. The custodian must assert in writing that all sensitive information has been securely removed from the device and no further sensitive information will be held on the device; or
   ii. The use of an alternative encryption technology is approved in writing by the University’s Chief Technology Officer is used.

3. An exemption may be authorised where the use of other necessary software or hardware conflicts with the use of the University’s managed encryption software. In such circumstances, either:
   i. The custodian must assert in writing that no sensitive information is or will be held on the device; or
   ii. The use of an alternative encryption technology is approved in writing by the University’s Chief Technology Officer.

4. The device is to be taken to another country, which legislates against the use of encryption. Options available in this situation will require individual scrutiny, however in general the preferred option in these circumstances would be to use a temporary, unencrypted loan laptop, containing only the files essential for the duration of the visit. Where such files contain sensitive information, written approval must be obtained from the University’s Chief Technology Officer, and Information Compliance Officer where personal data (as defined by the DPA) is to be included.

5. Any other scenario, not mentioned above: to discuss further please contact the University’s Chief Technology Officer, and Information Compliance Officer.

Where an exemption is granted, it will be subject to the following conditions:

1. It will be restricted to a specific single device, and is not “transferable”.
2. It will be valid for a maximum of one year, after which it must be renewed.
3. It may be revoked at any time by notice from the University’s CIO, CTO or ICO.
4. The device to which the exemption applies may be audited for compliance with the terms of the exemption at any time, by notice from the University’s CIO, CTO or ICO.
## Appendix B: Application for Exception to Encryption

### About you and your department

<table>
<thead>
<tr>
<th>Name</th>
<th>Email address</th>
<th>Extension</th>
<th>Department</th>
<th>Head of Dept.</th>
<th>Email address</th>
<th>Extension</th>
</tr>
</thead>
</table>

### About your laptop

<table>
<thead>
<tr>
<th>Make</th>
<th>Model</th>
<th>Serial number</th>
<th>Date of Purchase</th>
</tr>
</thead>
</table>

### About the information on your laptop

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes / No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is any personal data present on your laptop? If you are unsure, select “yes”. personal data is defined below.</td>
<td>Yes / No</td>
</tr>
<tr>
<td>If “yes”, please give details</td>
<td></td>
</tr>
<tr>
<td>Is any University financial data present on your laptop? If you are unsure, select “yes”.</td>
<td>Yes / No</td>
</tr>
<tr>
<td>If “yes”, please give details</td>
<td></td>
</tr>
<tr>
<td>Is there any other data present on your laptop whose disclosure could result in a financial loss to the University or might otherwise harm its reputation.</td>
<td>Yes / No</td>
</tr>
<tr>
<td>If “yes”, please give details</td>
<td></td>
</tr>
</tbody>
</table>

According to the Data Protection Act:

- **personal data** means data which relate to a living individual who can be identified –
  - (a) from those data, or
  - (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

  and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
<table>
<thead>
<tr>
<th>Reason for exemption</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. It does not meet the minimum standards necessary to run the University’s managed encryption software. Please supply full details.</td>
<td>Yes /No</td>
</tr>
<tr>
<td>2. There is a software conflict with the encryption software. Please supply full details</td>
<td>Yes / No</td>
</tr>
<tr>
<td>3. The device is to be taken outside the UK</td>
<td>Yes / No</td>
</tr>
<tr>
<td>4. Other. Please supply full details</td>
<td>Yes / No</td>
</tr>
</tbody>
</table>

I apply to have an encryption exemption for this laptop. I understand and agree that:

- If my laptop is not capable of supporting encryption, then I will not store any sensitive data.
- If there is any material change in the type of information to be present on my laptop, then I understand that this exemption is no longer valid, and I will have the laptop will be encrypted before such data is stored.
- My laptop may be audited at any time to confirm compliance with this exemption.

Name: ____________________________

Signature: ____________________________  Date: ____________________________

This application is endorsed by my Head of Department’s signature below.

Name: ____________________________

Signature: ____________________________  Date: ____________________________

Reviewed by CTO: ____________________________

Reviewed by ICO: ____________________________

Approved ____________________________

Authorised ____________________________

Constraints: ____________________________