Remote Access and Mobile Working Policy

**Document Status**

<table>
<thead>
<tr>
<th>Security Classification</th>
<th>Level 4 - PUBLIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.1</td>
</tr>
<tr>
<td>Status</td>
<td>DRAFT</td>
</tr>
<tr>
<td>Approval</td>
<td></td>
</tr>
<tr>
<td>Life</td>
<td>3 Years</td>
</tr>
<tr>
<td>Review</td>
<td>By June 2012</td>
</tr>
<tr>
<td>Owner</td>
<td>Secure Research Database Analyst</td>
</tr>
<tr>
<td>Retention</td>
<td></td>
</tr>
<tr>
<td>Change History</td>
<td></td>
</tr>
</tbody>
</table>
## Contents

Remote Access and Mobile Working Policy .......................................................... 1

Document Status ................................................................................................. 1

1. Introduction & definitions.................................................................................. 3
   1.1 Introduction ................................................................................................. 3
   1.7 Definitions ................................................................................................. 3

2. Scope & limitations ......................................................................................... 3

3. Available Remote Services ............................................................................... 4
   3.3 Staff ............................................................................................................ 4
   3.4 Students ...................................................................................................... 4
   3.5 External Users ............................................................................................ 5

4. Methods of Remotely Accessing Resources .................................................. 5

5. Remote Access for Systems Suppliers ............................................................ 5

6. User responsibilities, awareness and good working practices ....................... 6
   6.2 Responsibilities for data/ information accessed and processed during mobile
       working ........................................................................................................ 6
   6.3 Security of privately owned computers and other mobile working devices ... 7
   6.4 Security of IOE owned computers other mobile working devices ............ 8

7. Return of information assets to the IOE .......................................................... 8

8. Removal of Remote Access Rights .................................................................. 9
1. **Introduction & definitions**

1.1 **Introduction**

1.2 Mobile Working and remote access form an increasingly normal and accepted part of working life and study. It can provide benefits to the IOE and its employees and students by enhancing communication; supporting flexible working practices; enabling new modes of study, scholarship and research and facilitating the more efficient and effective use of time.

1.3 However, the rate of technological change and the proliferation of both physical devices for computing and virtual means of storage mean that data and information in digitised forms is increasingly at risk of being copied, stolen, lost or corrupted and the maintenance of authenticity, version control and other forms of record integrity is increasingly difficult to manage.

1.4 This combination of factors puts both the IOE, users of IOE systems and stakeholders dependent on IOE systems at risk of breaching ethical, legislative, regulatory and contractual requirements as well potentially contributing to poor and inefficient working practices.

1.5 The IOE and its IT services support secure, safe, accessible and available remote access and mobile working through its systems and policies, through the provision of essential technical controls and through raising user awareness and encouraging good working practices.

1.6 User awareness and responsible working practices are key elements of this policy.

1.7 **Definitions**

1.8 **Remote Access** - accessing IOE systems (e.g. email, Q Drive etc. see 3.3.1 and 3.4.1 for full lists) from outside of the IOE premises with an IOE owned, privately owned or publicly accessible home computer, laptop or smart phone or other similar devices.

1.9 **Mobile Working** - carrying out work (i.e. the creation, storage, processing and transport or transfer of data/information) as an employee of the IOE from outside of the IOE premises.

2. **Scope & limitations**

2.1 This policy applies to all remotely accessible systems and all authorised users and the data/information held, processed or controlled by the IOE.
2.2 It is important to note that the IOE does not make provision for all its IT systems and services to be made available remotely. In areas where the need for confidentiality or integrity is extremely high (such as when handling data classified as ‘Confidential’), remote access may not be appropriate.

2.3 Users should be aware that the availability and speed of remote access is subject to a number of external factors beyond the IOE’s control such as the effectiveness of any Internet Service Provider leased line, or any third party-supplied router, firewall, or anti-virus software in being able to create and maintain a connection to IOE systems and services.

3. Available Remote Services

3.1 Information on the relevant considerations for making a resource available remotely can be found on the IOE intranet page ‘Considerations when planning to make an IT resource available for remote access’:


3.2 Services made available can be broken down by category of authorised user:

3.3 Staff

3.3.1 Remote access is provided by default for all authorised staff users to the following systems and services:

- IOE Email
- CallPilot voice messages
- N drive (owner only)
- Q drive
- Library catalogue
- E Journals
- IOE Intranet

3.3.2 Other resources may be made available to limited groups of users if appropriate controls can be put in place relative to the required level of confidentiality of any information or data to be accessed and any potential impact on other systems.

3.4 Students

3.4.1 Authorised student users are given remote access to the following services:

- IOE Email/Live.edu email
- N drive
- Library catalogue
3.5 External Users

3.5.1 The default situation for external users (contractors, employees of other HE bodies working on IOE-led research projects etc) is they are given no remote access to IOE systems.

3.5.2 Individual resources may be made available to them on a case by case basis, where the request is properly authorised in writing by the head of a department or faculty, the request is appropriate for the data classification and an appropriate risk assessment of making the system or service available to remote access has been undertaken.

4. Methods of Remotely Accessing Resources

4.1 Remote access to resources is normally provided solely through the Institute’s https SSL Portal.

4.2 IT Services will consider and offer guidance, support and access and technical controls for other forms of remote access following assessments of their appropriateness to the IOE IT environment, affordability, their ability to be supported by IT Services, and their impact on the information security requirements of the IOE or of particular systems or services.

4.3 Current VPN client solutions are considered insecure, and are a threat to the confidentiality, integrity and availability of IOE data, due to the unverifiable security state of the computer making the VPN connection. VPN clients should therefore not be used, and all access to resources should be through the Portal.

4.4 Users must sign in to the Portal with a valid IOE Active Directory username and password. Anonymous, guest, generic or non-institute accounts will not be granted Portal access.

4.5 Methods used to access and process remotely available resources via the Portal must be concomitant with the data classification of the information being accessed. These are outlined in the Data Security Policy.

5. Remote Access for Systems Suppliers

5.1 The default position for new contracts with systems suppliers is that support and maintenance should be provided onsite, as opposed to being performed using remote access.
5.2 Providing suppliers with remote access involves making administrative accounts available outside IOE’s aegis of control, and allows the potential threat of uncontrolled changes and security breaches, putting the confidentiality and integrity of key systems and data at risk. Such an approach must be strongly discouraged in current contractual agreements, and must be discounted as an option when negotiating new contracts unless sufficient other controls can be put in place.

5.3 Existing systems suppliers remotely accessing IOE systems and services must submit a change control request before any upgrade, alteration or remedial work takes place.

5.4 User accounts for system suppliers must be kept disabled when they are not in use. A formal request must be made in writing to have the account enabled, and the request must stipulate when the account will be disabled again.

6. User responsibilities, awareness and good working practices

6.1 The primary responsibilities of employees, students and other users utilising remote access and/ or engaging in mobile working/ study are to:

i. know what data/ information they are using, storing or transferring
ii. consider what level of security classification should or does apply to it (for more information on this please refer to the Information Security Management Policy, the Data Security Policy and any current guidance on best practice).
iii. understand and act upon any particular contractual, ethical or other requirements attached to the information
iv. ensure that they devices they are working on and the data/ information they are processing are managed in accordance with this and related policies and guidance.

6.2 Responsibilities for data/ information accessed and/ or processed during mobile working

i. Highly confidential and high to medium risk data as defined in the Information Security Management Policy and Data Security Policy should not be created, stored or processed on privately owned computers.

ii. Appropriate precautions (see also 6.3 and 6.4, the Data Security Policy and any relevant Guidance Notes) and good practice should
be followed for all data and information created, stored or processed on mobile or home working devices or other media.

iii. Whilst strong controls can be put in place and/or reasonable assurances provided for user or IOE owned devices for remote access and mobile working, third party devices should not be considered secure and use of other privately owned devices (such as internet cafes) is strongly discouraged except in emergencies and in most cases will not be appropriate.

6.3 Security of privately owned computers and other mobile working devices

6.3.1 If users are utilising their own computers and other mobile working devices to carry out work for the IOE or undertake study at the IOE then they should ensure that to the extent it is appropriate to the device:

i. they keep themselves reasonably informed about current security threats to their device(s), software or systems and engage in safe web-surfing habits;
ii. they own and maintain up-to-date and well supported anti-virus and other internet security software;
iii. they install critical (such as operating system) software patches as soon as they become available;
iv. they enable a personal firewall to protect themselves from being hacked;
v. they consider full disk encryption as an option;
vi. they utilise other cryptographic (password) controls as appropriate;
vii. they regularly delete cached data;
viii. they do not respond to or enter data into unsolicited emails, texts, pop-ups, messages, surveys and other means of communication;
ix. they securely segregate their work/study from other users and according to the level of security required;
x. important data/information is regularly backed up or returned to IOE systems;
xi. portable devices are not left unattended or confidential data left clearly on the screen in public areas;
xii. locks and other physical security are utilised where feasible;
xiii. any security incidents (such as loss or corruption of data), concerns or problems that might impact on IOE work or systems are reported to IT Services and the relevant manager as soon as possible.
6.3.2 Users are whilst accessing IOE systems remotely or in relation to IOE data and information on their own systems subject to the Conditions of Use such as these are applicable.

6.4 Security of IOE owned computers other mobile working devices

6.4.1 If users are utilising IOE owned computers and other mobile working devices to carry out work for the IOE or undertake study at the IOE then:

i. If it was purchased and set up through IT services it is considered secure for access, however users should still:

- not respond to or enter data into unsolicited emails, texts, pop-ups, messages, surveys and other means of communication;
- keep themselves reasonably informed about current security threats to their device(s), software or systems and engage in safe web-surfing habits that accord with the Conditions of Use;
- securely segregate their work/study from other users and according to the level of security required;
- return the device to IT services for updates when requested or within a reasonable timeframe;
- regularly back up or return important data/information to IOE systems;
- ensure that portable devices are not left unattended or confidential data left clearly on the screen in public areas;
- ensure that locks and other physical security are utilised where feasible;
- always report any security incidents or problems to IT services.

ii. If it was not purchased and not set up through IT services then users should undertake the same actions as detailed in 6.3.1. Departments should maintain an asset register of IT equipment not purchased or set up via IT services recording the model, serial number and name of the device as well as the names of authorised user(s).

6.4.2 Users using IOE owned IT equipment (PCs, Laptops etc.) are fully subject to the Conditions of Use.

7. Return of information assets to the IOE

7.1 All IOE-owned devices/equipment and information/data must be returned to the IOE upon termination of employment, contract, or agreement.
7.2 IOE IT equipment should be returned at the scheduled times and or on request by IT services for critical system updates and routine maintenance.

7.3 Before returning the end user device to IT Services, users should remove their own personal (non-work) data from the device.

8. Removal of Remote Access Rights

8.1 Rights to remotely access IOE systems may be changed or removed by IOE from any authorised or unauthorised user at any time if a breach of the conditions of use is evident or that user’s access is compromising the confidentiality, integrity and/or availability of the IOE’s systems or services. Users will be informed of the reason for the change of access rights as soon as is feasible unless there are substantive reasons not to do so.

8.2 The remote access rights of all employees, contractors and third party users shall be removed upon termination of employment, contract, or agreement.