Acceptable Use of Information Technology Policy

1. Introduction

1.1 This policy is part of the Library's **Information Security Policy** and forms part of the Library's **Information Risk Management Framework.** It replaces the previous Electronic Communications Security Policy.

1.2 This policy covers:

- Responsible and appropriate use of the Library's electronic communication systems and equipment – including the Library's Information Technology ("IT") infrastructure, computer systems, telecommunications, mobile communications, storage and computing facilities whether used on site, off site or accessed remotely.
- Acceptable usage of British Library owned technology for processing, storage and transmission of data and;
- Acceptable usage and application of electronic communications of all forms both internal and external, including email, intranet and internet facilities.

1.3 The policy is comprised of this main umbrella document and eight sub policies to which it refers, as follows:

- Acceptable Business Use
- Acceptable Personal Use
- Unacceptable Use of IT
- Offensive & Discriminatory Material
- Hardware & Software
- Confidential, Personal and Sensitive Data
- Content Filtering, Monitoring and Interception.
- Copyright, Intellectual Property and Patented Material

1.4 This policy must be understood and accepted by all members of staff (including anyone undertaking work or services for the Library which involve the use of Library IT facilities). Intentional breach of this policy may result in disciplinary action being taken in accordance with the Library's **Disciplinary Policy**.

1.5 Formal acceptance of this policy by all Authorised Users ("Users") is required before the Library will grant them access to its electronic Systems. There will be initial or periodical initiatives to check awareness of and compliance with this policy, which will require appropriate and successful participation from Users as appropriate.

1.6 This policy does not cover all aspects of the use of Social Media and staff should also refer to the Library's **Social Media Policy** and associated guidance.

2. Objectives

2.1 This policy aims to facilitate proper use of the Library's electronic systems and set out the consequences of misuse of those systems. By doing so the Library expects to reduce the likelihood of security incidents and exposure to legal liability arising from the use of electronic Systems by Library staff and visitors.

3. Definitions

3.1 **Authorised User ("User") –** Any individual who is permitted access to British Library buildings and systems during the course of their work for the British Library. This includes:

Permanent staff employed directly by the British Library and on the British Library Payroll and recruited by Human Resources;

- Third party staff hired indirectly through a third party listed on the British Library's preferred supplier list. This includes agency staff;
- Consultants, contractors and other temporary workers engaged indirectly through procurement contracts;
- Voluntary staff and interns.

3.2 **System -** Computer based information technology (IT) hardware, software and networks which support the day to day operations of the British Library. This definition includes all electronic communication equipment including (but not limited to) desktop computers, laptops, memory sticks, telephones and smart phones, and other electronic devices. This definition also includes all electronic communication facilities, including (but not limited to) email, the internet, instant messaging, social media, and other web publishing tools.

3.3 **Third Party -** Any external organisation or individual who is not a member of the Library staff, for example service providers, external IT maintenance and support staff, contractors or consultants. This includes external individuals and agencies not working under the instruction or on behalf of the Library, such as regulatory authorities and law enforcement agencies.

3.4 **Visitor –** Any member of the general public who visits the Library premises as a Reader, customer or guest.

3.5 Any IT terms used in this policy shall, in the event of any disagreement, be understood to have the meaning given to them in the Library's **Information Security Policy** and **Information Security Manual**.

4. Scope

4.1 This policy (including its sub-policies) applies to all Users of Library Systems, who are required to comply with this policy and its associated processes, controls and guidelines.

4.2 This policy applies to the use of all Systems and any related facilities and equipment at any time, and whether onsite (at any Library site, including in the Reading Rooms) or offsite (including at home and during travel).

5. Acceptable Use of Information Technology Policy

5.1 User responsibilities for British Library Systems have been defined in this policy (and its sub-policies) so as to take into account the Library's needs for security, attainment of Corporate Business Plans and strategic goals, efficient information management, compliance with employment law, and staff expectations of reasonable personal use.

5.2 The Library provides standardized hardware and software applications for the use of all Users. Any further requirement for the provision of, or access to, additional hardware and software must be justified by a legitimate and demonstrable business need.

5.3 This policy is supported by a number of sub-policies. This will enable the Library to update details of the policy in response to legal or technical changes without having to review and revise the entire Acceptable Use policy.

6. User Responsibilities

6.1 Users should be aware that IT equipment, software and Systems are provided primarily for the purpose of work. Uses of IT hardware and software that are specifically permitted for business use can be found in the **Acceptable Business Use Sub-Policy.**

6.2 Users must ensure that any personal use of Library IT equipment, software and Systems complies with the requirements set out in the **Acceptable Personal Use Sub-Policy**.

6.3 Certain uses of Library IT equipment, software and Systems are explicitly forbidden. Users must not use Library IT facilities in such a way as to waste Library time or resources, compromise the Library's security, or harm the Library's reputation. Users should make themselves fully aware of the specific details of the **Unacceptable Use of IT Sub-Policy.** Users who breach this policy may be subject to disciplinary measures.

6.4 Users are strictly prohibited from using Library IT equipment, software & Systems to intentionally access, send, solicit, store or use any material in any format which could be regarded as offensive or discriminatory. Users should make themselves fully aware of the specific details of the **Offensive & Discriminatory Material Sub-Policy.** Users who breach this policy may be subject to disciplinary measures.

6.5 Users should be aware that the Computer Misuse Act 1990 (as noted in warning messages during log-on to the Library's network) applies to the usage of all Library IT equipment, software and Systems, and that acceptance of this policy (for example by contract with the Library as an employee, volunteer or supplier) also acknowledges this fact.

6.6 All Users are responsible for the security of the Systems and information entrusted to them to enable the fulfilment of their role. This includes a duty of care to use the facilities provided in a responsible way so as not to cause harm to themselves, colleagues, the Library and its Collections, Third Parties, or the facilities provided. For shared hardware, the User named in the IT hardware asset register as the business owner is primarily responsible for ensuring that the device is protected and used in an appropriate manner by other colleagues, although all Users remain responsible for their own use of any of the Library's IT equipment. Users are required to comply with the provisions of the Library's **Information Security Policy,** particularly in relation to the protection and use of passwords. Users are directed to the Library's published guidance on **Choosing Better Passwords.**

6.7 Users may only process and store information belonging to the Library on Library Systems, software and hardware, unless specifically authorised to do otherwise by IT Operations or under contractual arrangement. Further information can be found in the **IT Hardware & Software Sub-Policy.**

6.8 All Users must comply with, and assist with the operation of, any controls deemed necessary by IT Operations to protect the security, integrity and efficient functioning of the Library's Systems, and must take reasonable precautions to prevent accidental or deliberate interference with the security, integrity and functioning of those Systems. Further information can be found in the **IT Hardware & Software Sub-Policy.**

6.9 All Users must comply with all legal requirements imposed on the use of information and IT equipment and Systems, and pay specific attention to the requirements of the **Confidential, Personal and Sensitive Data Sub-Policy**. Users should be careful that they do not infringe any intellectual property (e.g. copyright) in their work intended for transmission to Third Parties or for general publication. It is expressly forbidden to copy, download or transmit material in a deliberate attempt to bypass the intellectual property rights of either a Third Party or the Library itself.

6.10 Users have a general right to privacy at work. The Library is mindful of this right but also needs to ensure the effective operation of its work and to safeguard the Library itself, its Collections, its staff and the rights of third parties. Users should therefore be aware that the Library operates content monitoring and filtering software to enable the security of our Systems and the protection of the Library, its Collections, its staff and its third party stakeholders. If necessary (due to suspected serious misconduct or other risks) the Library may instigate whatever targeted interceptions of communications made with library equipment, software or Systems, or detailed monitoring of IT is necessary to ensure that our security is not compromised and that relevant legal requirements are complied with. In these instances the monitoring will only be carried out in accordance with the provisions of the Library's **Content Filtering, Monitoring and Interception Sub Policy** following a properly authorized Privacy Impact Assessment.

6.11 Line Managers must ensure that their staff are aware of the requirements of this policy, and must ensure that the work of their team or department complies with the requirements of this policy.

7. Ownership & Review

7.1 IT Operations is responsible for the implementation, support and security of the Library's computer systems, software and networks and will provide best practice advice and support to line managers and all staff on these areas.

7.2 The IT Security Officer has responsibility for ensuring the maintenance, regular review and updating of this policy, supported by HR and CIMU.

7.3 Line Managers are responsible for ensuring both that Users are aware of this policy and that this policy is applied within their own area. Both Line Managers and other Users should seek advice as necessary from the IT Help-Desk if they are unclear as to the application, interpretation or requirements of this policy.

7.4 This policy will be reviewed by the Corporate Information Governance Group on an annual basis. Any changes recommended will be signed off by the Executive Leadership Team after appropriate consultation with Trade Union Side.