St Georges, University of London

Encryption Policy

1. Purpose and scope

This policy applies to all University staff that handle University data and confidential information and sets out the framework within which the University will manage the security of the information for which it is responsible, maintaining an appropriate balance between accessibility and security. This document sets out the University's policy on processing high risk data and sensitive information off campus or on an external network, including the use of portable and mobile equipment. Its aim is to ensure that the University complies with data protection laws and other legal obligations and that University data is protected from unauthorised access, dissemination, alteration or deletion.

1.1 The University recognises the need for its staff to be able to disseminate, store and transport the information they require in order to carry out their work.

1.2 The University also recognises that the information it manages must be appropriately secured in order to maintain its reputation for trustworthiness, to protect against damage and/or distress being caused to those that entrust us with their data, to protect the institution from the consequences of breaches of confidentiality including possible legal and financial consequences , to avoid failures of integrity or interruption to the availability of that information and to comply with the law and any applicable contractual agreements.

1.3 This policy applies to all information for which the University has a legal, contractual or compliance responsibility, whether that information is stored or processed electronically or by other means.

1.4 This policy applies to the use of mobile devices (e.g. laptops, tablets, and smartphones), portable storage media (e.g. USB memory sticks, portable hard drives, CDs or DVDs), remote computers, or other forms of communication (e.g. websites, email and instant messaging).

1.5 This policy applies to all staff or any other person or organisation having access to University data.

2. Roles & Responsibilities

Directors (Information Asset Owners)

To ensure that an appropriate security classification is applied to the Information they are responsible for, and that encryption of high risk data and sensitive information is applied where required.

To ensure that the business rules covering access rights to the service are defined and maintained, and that they are compatible with the security classification of the underlying information.

To ensure that the information security risks for the service are identified, assessed and addressed prior to implementation, and reviewed at regular intervals thereafter.

To ensure that information assets are effectively managed in accordance with the data protection principles and Data Protection Policy.

To assist with any Information Security Incident as part of the Information Security Incident Response procedures.

To ensure that their staff are made aware of this policy and that breaches of it are dealt with appropriately.

University staff

To assess the need for encryption, based on requirements set out in this policy and apply appropriate security measures as needed. To comply with the Regulations on the Use of IT Facilities. To complete all required training and follow related policies and guidance.

To report any breaches or suspected breaches of Information Security in accordance with the Information Security Incident Response Policy.

To inform IT Services of any potential threats to Information Security.

3. Consequences of Non-Compliance

3.1 Failure to comply with this policy may result in the University revoking your access to the University's systems, whether through a device or otherwise. It may also result in disciplinary action being taken against members of staff up to and including dismissal. In the case of breach of this policy by a contractor, worker or volunteer, it may lead to the termination of the engagement. This will apply whether the breach occurs during or outside normal working hours and whether the breach takes place at your normal place of work.

4. Requirements and Key Principles

The following key principles underpin this Policy.

4.1 If processing personal data on external networks or devices staff must first consider whether anonymising the information to obscure the identity of the individuals concerned would be possible.

4.2 University data must wherever possible be stored and transmitted within University managed systems using University Virtual Private Network (VPN) where available.

4.3 If high risk or sensitive information is to be processed off campus or on an external network, then it must be stored and transmitted in an encrypted form. This includes the encryption of files sent by email, data in transit held on portable hard drives, and in the case of websites or e-commerce, the use of encrypted transmission protocols such as SSL. There are exceptions where access or transmission of high risk or sensitive information is being conducted using University managed systems such as University managed email and cloud services.

4.4 Staff should not use non-IT centralised third party hosting services, like Dropbox or Google mail/storage, when processing high risk or sensitive information. Seek advice from IMPS or IT regarding University approved alternatives (such as One Drive) or to seek authorisation for use by exception.

4.5 Staff should not process high risk or sensitive information in public places. When accessing your email remotely, exercise caution to ensure that you do not download unencrypted high risk or sensitive information to an insecure device. Please refer to University Policies on remote working for additional requirements for working off campus.

4.6 When sending encrypted data outside the UK, staff should have regard for the regulatory regime in the destination country. Be aware when travelling abroad that government agencies may require you to decrypt information on entering or exiting a country. Wherever possible avoid travelling with high risk or sensitive information. Seek advice from IT if required.

4.7 Third party hosted data, for example where external suppliers are used, including software as a service, cloud hosted solutions and third-party web-based applications will be subject to due diligence check to ensure they can afford an appropriate level of security for personal data. When requested you may be required to obtain information pertaining to supplier security and encryption measures on request.

4.8 All University owned laptops, smartphones and tablets shall be encrypted unless in exceptional instances where this is not deemed necessary

4.9 The University's centrally approved encryption solutions will be used, and all encryption keys, passwords, passphrases or other keys must be held centrally to ensure accessibility of data when required.

4.10 All staff using personally owned devices must comply with the requirements of the Bring your own device (BYOD) Policy.

4.11 Staff should wherever possible avoid the storing of high risk or sensitive information on personally owned devices. Where this is unavoidable, staff must encrypt the device using IT approved encryption standards. Staff will be wholly responsible for the safe management of their encryption keys, passwords and any other means of access; IT will be unable to recover lost passwords for personally owned devices and staff should be aware that loss of passwords or encryption keys could render data inaccessible. For this reason, you must ensure that copies of the data are maintained on University systems to protect against risks posed by data becoming inaccessible.

4.12 Portable devices such as USB sticks, portable hard drives, and recording devices are at higher risk of loss or theft so additional care must be taken to protect the physical security of these devices.

4.13 Wherever available, device encryption should be used ensuring that encryption keys, passwords and any other means of access are stored securely on University networks.

4.14 Alternatively, encrypt files that will be stored on the device.

4.15 Encryption is a mandatory requirement for any portable devices/removable media that will be used to store or transfer high risk or sensitive information.

4.16 Avoid sending high risk or sensitive information externally by email or using email to store such information. If you must use email to send this sort of information externally, encrypt it prior to sending.

4.17 If you are sending unencrypted high risk or sensitive information to another internal University email account, to include any accounts issued by the University, take extra care that you have the correct recipient, indicate in the email subject line that the email contains sensitive or confidential information so that the recipient can exercise caution about where and when they open it. This includes those invited to view documents within cloud-based storage e.g. One Drive. Password protection for internally transmitted documents is advisable and may be mandated by the DPO in instances of recurrent errors involving incorrect recipients.

4.18 Ensure that any third party working with any University data that involves high risk or sensitive information handles it in accordance with this policy.

4.19 Encryption keys, e.g. passwords, must not be communicated within the same channel as the encrypted data, for example, do not send a password within the same email as the encrypted information, or a USB stick together with the password.

4.20 Suspected or confirmed compromises of personal data (irrespective of classification or being high risk) or sensitive information must be reported to the IMPS team promptly in line with the requirements of the University Information Security Incident Response Policy. Lost or stolen University issued IT devices should also be reported to IT immediately.

4.21 Use the University's central and secure shared drives to store and access high risk and sensitive information wherever possible; this helps to ensure that only legitimate users have access to it as well as ensuring it can be readily accessed.

4.22 Use the IT-authorised remote access facilities (such as VPN) to access University data on the central servers instead of transporting it on mobile devices and portable media wherever possible.

5. High Risk data and sensitive information is

- Any set of data relating to more than 50 living, identifiable individuals, including, but not limited to, students, staff, alumni, research participants.

- Any set of data relating to 10 or more living, identifiable individuals that could be used for fraud or identity theft, including, but not limited to, bank account or credit card details, national insurance number, personal contact details, date of birth, salary

- Information relating to 10 or more members of staffs' performance, grading, promotion or personal and family lives.

- Information relating to 10 or more alumni/students' programmes of study, grades, progression, or personal and family lives.

- Any set of data relating to 5 or more living, identifiable individuals' health, disability, ethnicity, sex life, trade union membership, political or religious affiliations, or the commission or alleged commission of an offence.

- Information relating to identifiable research participants, other than information in the public domain.

- Information that would be likely to disadvantage the University in funding, commercial or policy negotiations.

- Confidential information critical to the business continuity of the University, and information held in business-critical applications

- Any information or data that is subject to non-disclosure agreements or any other contractual confidentiality obligations

- Information provided to the University subject to contractually binding requirements governing the use of Encryption.

- Finance data held in Agresso and any payment card data covered by PCIDSS security requirements.

- Health records of any living, identifiable individual.

- Discussion papers and options relating to proposed changes to high profile University strategies, policies and procedures, such as the University's undergraduate admissions policy, before the changes are announced.

- Security arrangements for high profile or vulnerable visitors, students, events or buildings while the arrangements are still relevant.

- Information that would attract legal professional privilege.

- information that is marked as confidential.