UNIVERSITY OF SUSSEX

IT Services

IT REMOTE WORKING POLICY

1. OVERVIEW AND PURPOSE

1.1 The University of Sussex is committed to enabling and facilitating effective off-campus (remote) working, supported by ITS solutions and appropriate policies.

1.2 The University has a number of policies in place that detail requirements in relation to information security and adherence to data protection legislation. This policy outlines how these should be applied within the context of remote working so that information and personal data remain secure and adequately protected.

1.3 This policy outlines additional risks associated with working remotely and associated steps that should be taken to mitigate these risks, making clear responsibilities associated with remote working.

2. SCOPE

2.1 This policy applies to any University business carried out off-campus (in public or private spaces), either via University-owned or personal devices, including mobile devices.

2.2 This policy must be adhered to by all individuals carrying out University business remotely, either remunerated or not, including:

- Senior managers, officers, and directors;
- Employees (whether permanent, fixed-term, temporary, or casual);
- Contract, seconded, and agency staff;
- Volunteers, apprentices, and interns; and
- Others associated with (i.e. performing services for or on behalf of) the University, for example contractors and consultants.

2.3 This policy does not apply directly to students, unless they are carrying out University business remotely (e.g. as an employee, volunteer, etc.).

2.4 This policy refers only to remote working considerations within the context of IT, information security, and data protection; guidance and advice relating to other matters (e.g. contractual arrangements, flexible working, health and safety) should be sought directly from the relevant team(s) at the University.

3. RESPONSIBILITIES

3.1 All individuals to whom this policy applies (outlined in 2.2) must adhere to this policy and related guidance; other individuals/parties with specific responsibilities related to this policy are outlined below.

3.2 Information Governance Committee (IGC)

3.2.1 IGC, having oversight of matters relating to information security and data protection at the University, is responsible for ensuring that the necessary processes and systems are in place to support this policy.

3.2.2 IGC is responsible for ensuring that the policy is regularly reviewed and remains fit for purpose.

3.3 Senior Information Risk Owner (SIRO)

3.3.1 The SIRO is responsible for driving a culture that values and protects information and for ensuring that information risks associated with remote working are managed and mitigated through appropriate policies and procedures.

3.4 Director of IT Services

3.4.1 The Director of IT Services has overall management of information security policies and is responsible for ensuring that information systems and technologies are implemented and available in a way that supports the security of information in the context of remote working.

3.4.2 The Director of IT Services is responsible for ensuring that adequate technical advice and guidance is made available to staff.

3.5 Data Protection Officer (DPO)

3.5.1 The DPO is responsible for monitoring compliance with data protection requirements and for advising on data protection obligations under this policy.

4. POLICY

4.1 Additional Risks of Remote Working

4.1.1 Information and personal data processed whilst working remotely must be safeguarded to the same extent that it is when working on campus.

4.1.2 Conducting University business outside of the University campus can carry with it additional risks, however, which must also be considered when working remotely. Examples of such risks include:

- The risk of work being seen by unauthorised individuals for example in public or personal spaces;
- The use of devices not supplied by the University;
- Loss or theft of devices and/or credentials;
- File storage or processing personal data outside of the University network or systems;
- Insufficient password protection, privacy settings, or anti-virus protection;
- Unauthorised access to remote gateways;
- Use of outdated software;
- Phishing risks and use of personal email;
- Inappropriate recording or use of video conferences and teaching activities; and
- Inadequate legal safeguards in other jurisdictions.

4.1.3 This policy serves to draw attention to responsibilities and obligations outlined in existing University policies (linked at the end of this policy) designed to ensure security and compliance, as well as to highlight additional measures that must be taken to mitigate the additional risks of remote working.

4.2 Data Protection

4.2.1 All processing of personal data done in the course of working remotely must adhere to the data protection principles and other requirements of data protection legislation and the University's Data Protection Policy.

4.2.2 Personal data breaches occurring in the context of remote working must still be reported to the University's Data Protection Officer via the published process.

4.3 Information Security

4.3.1 All University business carried out remotely must adhere to the principles and requirements laid out in the University's Information Security Policy and associated policies and guidance linked at the end of this policy and referred to throughout.

4.4 ITS Support

4.4.1 ITS should be the first point of contact should any issues or malfunctions arise relating to University-owned equipment, University-provided email, or University-approved/installed/licensed software/solutions.

4.4.2 If the remote worker uses their own devices, they will be responsible for any repairs or technical support relating to the device itself. University equipment will be repaired by IT Services.

4.4.3 Support for IT Services operates during normal business hours and details of how to contact the IT Service desk can be found on the University's ITS web pages.

4.5 Equipment and Systems

4.5.1 An individual's remote working set-up should be discussed in the first instance with their line manager, to determine what equipment, systems, and solutions should be used, based on the nature and quantity of the work being undertaken, as well as the budget of the respective School or Division.

4.5.2 Equipment and systems or software provided by the University, as well as the University network, should be primarily used for business purposes and only by the University's remote worker.

4.5.3 Whether conducting University business on a personal or University-owned device, individuals must only use ITS-approved technologies and software, which should all be kept up to date.

4.5.4 No software or non-standard hardware should be installed on a University-owned device without authorisation from IT Services, and users must allow installation / updates of any University-installed programs and software, including anti-virus software.

4.5.5 Individuals using University-owned devices are responsible for the safekeeping and protection of these devices and reasonable care should be taken to prevent or reduce the possibility of loss or theft of such devices. Any asset or registration numbers on University-owned devices must not be removed or defaced.

4.5.6 Individuals using their own equipment and devices should refer to the BYOD Policy and Guidance Notes on the Regulations for Use of Information Technology to ensure that they have the correct security measures in place for conducting University business.

4.6 Online Teaching and Learning

4.6.1 Individuals engaging in teaching activities as part of their University business must adhere to the University's Policy on the Recording of Teaching Activities and Other Uses of Panopto and must follow any guidance published by the TEL team in relation to online teaching and the use of technologies.

4.6.2 The recording of teaching activities by individuals other than the academic is not permitted without the prior consent of the academic and other individuals involved, unless it is a reasonable adjustment as part of a student's disability learning plan.

4.6.3 When delivery is being recorded, this should be highlighted in advance, details should be provided as to how the recording will be used.

4.6.4 Recordings may only be used for the purpose for which the recording is made – usually to support teaching and learning and for the purpose of personal study.

4.6.5 Recordings must not be reproduced or distributed to any third party and must not be made available on external websites or social media channels.

4.7 Online/Video Conferencing

4.7.1 When using online/video conferencing to conduct University business, individuals should use only University approved/supported technologies and must adhere to all guidance issued by ITS in relation to their use.

4.7.2 All online/video conferencing software must be kept up to date.

4.7.3 If a video conferencing meeting or session is being recorded, this should be highlighted in advance, with details provided as to how the recording will be used.

4.8 File Storage, Access, and Transfer

4.8.1 Any files relating to University business should not be stored locally on the device's own drive or desktop (whether it is a University-owned or personal device).

4.8.2 Files should be stored on the University's network / using University-approved solutions (e.g. Box) with access restricted to only those requiring it.

4.8.3 The sharing and transferring of files must be done in accordance with the University's Data Protection Policy and Information Security policies.

4.8.4 Paper files used for the purposes of remote working which include personal data or sensitive information must be stored and disposed of securely, in line with the University's Data Protection Policy and Information Classification and Handling Policy.

4.9 Use of Email (& Telephone)

4.9.1 All University business conducted via email should be carried out using the individual's University of Sussex email account only, and emails should not be forwarded from this account to a personal account.

4.9.2 University business carried out via telephone should be conducted using a University-owned mobile phone. Individuals without a University-issued telephone should use alternative University/ITS-approved solutions (e.g. Skype, Microsoft Teams).

4.10 **Breach of Policy**

4.10.1 Where there is deliberate misconduct or behaviour amounting to a wilful breach of this policy, or gross negligence causing a breach of the policy, the matter may be considered under the University's Disciplinary Procedure under Regulation 31.

5. RELATED EXTERNAL GUIDANCE AND GOOD PRACTICE

5.1 Information Commissioner's Office working from home guidance: https://ico.org.uk/for-organisations/working-from-home/

5.2 The National Cyber Security Centre (NCSC) have also issued guidance about working from home: https://www.ncsc.gov.uk/guidance/home-working

Review / Contacts / References	
Policy title:	IT Remote Working Policy
Date approved:	28 July 2020
Approving body:	Information Governance Committee
Last review date:	28 July 2020
Revision history:	July 2020 - First version
Next review date:	July 2021
Related internal policies, procedures, guidance:	Information Security Policies Information Security Policy Bring Your Own Device Policy Cryptography Policy Information Classification and Handling Policy Regulations for Use of Information Technology Guidance Notes on the Regulations for the Use of Information Technology (Acceptable Use) Data Protection Policy Data Protection Email Guidance Online/Video Conferencing Guidance TEL Guidance Policy on the Recording of Teaching Activities and Other Uses of Panopto ITS Top 10 Security Tips
Policy owner:	IT Services
Lead contact / author:	Pete Collier - Assistant Director, Strategy and Architecture (ITS)

	Karen Blackman - Information Manager (Information Management and Compliance)