

Remote Working Procedure

Enabling Policy Statement; Executive Owner; Approval Route:	Our Colleagues – Chief Operating Officer – Operations Committee
Is the Procedure for internal use only (Non-disclosable)?	Disclosable
Associated Policy Statements:	Our Data Our Safety
Authorised Owner:	Human Resources Director
Authorised Co-ordinator:	Associate Director (People Services)
Effective date:	31 March 2025
Due date for full review:	31 March 2028
Sub documentation:	N/A

Approval History

Version	Reason for review	Approval Route	Date
1.0	3 Yearly review and migration to the POPP governance structure	Operations Committee (Chair's Action)	31 March 2025

1. Purpose

This procedure has been developed to protect sensitive or valuable data and maintain the overall security of University data and equipment whilst employees are working remotely. In addition, this procedure recognises and defines the duty of care of the University to the remote working employees in regard to their health and safety and fair treatment.

Employees must ensure security of information and systems accessed through mobile and remote working arrangements are given due consideration. This procedure emphasises the importance of staff understanding the University's current Information security policies and procedures and each individual's responsibilities in relation to these which must be adhered to at all times.

Information that is related to and can identify an individual is called personal data and is protected by the principles of the UK General Data Protection Regulation 2016/679 and Data Protection Act 2018.

2. Scope and Exceptions to the Procedure

In principle, any job role at the University of Surrey or its subsidiaries could be considered for remote working. Nevertheless, it is clearly the case that some activities can only be adequately carried out on-site, whilst others may be carried out equally or even more effectively at a remote location – usually the employee's home.

Where a role is not already working in a remote capacity, for it to be considered for remote working, the employee should discuss blended working with their line manager who will consider the effectiveness of the role being performed off site and any impact of this.

For a role to be considered for regular/permanent remote working, the employee must submit a flexible working request to their line manager who will consider the request under the University's Flexible Working Procedure.

The Remote Working Procedure should not be used as an alternative to caring for dependents. For dependency leave, please refer to the University Leave Procedure.

This procedure does not form part of any employee's contract of employment. It may be amended from time to time with appropriate consultation with recognised trade union representatives.

3. Definitions and Terminology

Remote working: a formal work arrangement that permits an employee to conduct all or some of their work at an approved alternative worksite such as the home or in office space near to the employee's home on a formal permanent basis or for a formal agreed period of time.

Blended working: otherwise known as hybrid working. This is a more informal work arrangement that means that employees undertake some of their work on campus and some remotely, the exact balance will vary depending on roles and responsibilities

4. Procedural Principles

Where an existing remote working pattern is not in place, a proposal to conduct remote working needs to be submitted to the line manager and carefully reviewed in terms of: the cost of providing equipment; health and safety and communications considerations; security, data protection, and other legal issues; working and reporting relationships and any requirements to attend work to perform the duties of the post.

4.1 Personal Security

For the maintenance of personal security, the University strongly advises against any external work contacts visiting an employee when they are working at home and that such visits should take place on the University premises wherever possible.

For the employee's own security, it is also recommended that employees who are remote working should:

- Not release any personal data or information to external contacts such as home address or personal telephone number
- All employee's remote working business lines should be ex-directory
- Always ensure that colleagues are aware of the remote working employee's whereabouts and that you are able to be contacted within your contractual working hours.

4.2 Security of Equipment and Data

To ensure safety and security is maintained at all times, a separate allocated room should be used for remote working, where possible.

University provided IT equipment has a range of security measures enabled to make home working safer. Do not use personal devices for storing, accessing or transmitting personal or commercially sensitive information. Further information around the rules and guidance can be found in the University's *Use Your Own Device* procedure.

The *University Information Security* procedure should be adhered to when remote working; this includes locking a device when not in use, ensuring that data is encrypted in the event of device loss and not disclosing any passwords, PINs or encryption keys. It is the responsibility of the remote worker to safeguard and protect any University information that they hold. Remote workers must have an understanding of digital risks, use secure working practices and apply encryption and back-up procedures as appropriate. If the remote worker is not confident in this area, they should seek assistance from the IT User Support team prior to working remotely.

Digital information must only be downloaded or uploaded over a secure connection. WiFi networks offered to travellers at airports, hotels, coffee shops and on public transport are generally insecure and extra measures must be taken to safeguard against information loss. Surrey's VPN service provides a secure channel for data transfer over insecure networks and should be used by remote workers when interacting with University resources. This includes but is not limited to use with desktops, laptops, tablets and smartphones. Please visit the VDI service, workspaces.surrey.ac.uk for a secure connection to internal surrey resources.

4.3 Health and Safety

The underlying principle of this section is that the standards of care towards remote workers should be equivalent to that of employees working on the University's premises. It is, therefore, essential that the conduct of University business from an employee's home, or elsewhere, does not adversely affect the health and safety of the individual or others.

In exercising this duty of care, the University has undertaken a general risk assessment for remote working: [Remote Working Risk Assessment](#)

This assessment covers the keys risks associated with working remotely, and the control measures employees should adopt to protect themselves from harm.

In accordance with the *Health and Safety (Display Screen Equipment) Regulations 1992 (as amended)*, employees must also conduct a Display Screen Equipment (DSE) self-assessment within the first week of remote working and confirm in writing to their line manager that this has been completed. This will ensure that both equipment and working practices at the remote location are not presenting any significant risk of harm. For working from home, the employee will take primary responsibility for ensuring safe and healthy working conditions in their home environment, bringing to the attention of their line manager any significant risks identified.

If further clarification or advice is needed, the manager and employee should consult with their Health and Safety Manager/Advisor or HR Department representative.

The University has the right to refuse to allow remote working on the grounds of health and safety.

4.4 Equipment

The line manager will discuss and agree with the employee prior to commencing remote working, what equipment and IT requirements will be needed to enable the individual to work effectively from home. Unlike blended working, due to the formal agreement for remote working, any equipment necessary will be provided by the University who will bear the full cost of delivery and installation. The equipment will remain the property of the University at all times.

In the event of University equipment malfunctioning or inoperability, the IT department will, in the first instance, provide email and telephone support line to assist the remote worker to identify and remedy the fault. If the fault persists, the IT department will discuss arrangements to recover and replace equipment at the earliest opportunity.

With regard to the equipment, the remote worker will be expected to:

- Take reasonable care of the equipment;
- Take all reasonable steps to minimize the risk of theft or damage to University property and paperwork whilst these items are away from University premises;
- Use it only for work purposes and in accordance with any operating instructions as defined in the University Information Security procedure;
- Comply with software licensing Terms and Conditions;
- Return to the University, the equipment at the end of the Remote working arrangement.

In the event that equipment becomes obsolete, the cost of recovering the items from the remote worker's home will be covered by the respective department.

The University will only need access to the employee's home when setting up/repairing/collecting equipment or if a disciplinary matter has arisen that requires access to the employee's home. Any access requirements will be notified to the employee with reasonable notice.

In the event the employee moves house under the Remote Working agreement, the employee must make the line manager aware so that IT are able to collect and set up equipment at the new address. All other terms and conditions remain the same.

4.5 Financial Matters and Insurance

Employees working remotely are responsible for the safekeeping and protection of University-owned electronic devices that have been issued or loaned to them and reasonable care and due diligence must be taken to prevent or reduce the possibility of loss or theft of University-owned electronic devices.

Remote working employees are required to be aware of the environment in which they are working and apply appropriate common-sense measures to protect University-owned equipment and University data on both University-owned and privately-owned devices in accordance with the University's *IT Security* procedure.

The University Insurance policy excess for University equipment is £5,000 and therefore any damaged or stolen (in the case of forced entry) equipment replacement costs would be liable by the relevant department of the employee. Equipment in transit left in a stationary vehicle must be locked securely out of site. Remote Working employees will be responsible for the cost of equipment which is damaged or lost due to their own negligence. It is advisable, for this reason, that remote working employees clarify whether their personal insurance will cover them for damage or loss due to negligence.

Losses of, or damage to, University-owned electronic devices may be investigated in accordance with the University's Disciplinary Procedure.

The University will not reimburse any expenses incurred through remote working apart from items such as postage and packaging which can be reimbursed by using the University expenses system.

The University will not reimburse an employee for costs incurred whilst remote working through the use of electricity.

Employees will be reimbursed in full for travel expenses wholly, necessarily and exclusively incurred in the course of the University's business, through the online expenses system. For further clarification on the reimbursement of expenses, please refer to the University Staff Expenses Procedure.

Employees are advised to seek clarification and advice from their relevant mortgage/insurance provider with regards to Remote Working and the impact it may have on their insurance and cover / payments.

4.6 Terms and conditions

The underpinning principle is that remote working employees will be no worse off than office-based employees when conducting their work. For example, remote workers will be eligible to attend all appropriate training courses in the same way as office-based employees.

Remote working employees, maintain their existing terms and conditions of employment apart from their designated place of work which changes from the University to the remote worker's defined remote site.

Prior to commencing Remote Working the employee and line manager should agree on the working pattern of the employee and the times they will be available for contact. The employee should be made aware by their line manager that they will be required to visit campus on occasion as required by their line manager or department. Desk space will be provided for this visit.

If either party request the remote working arrangements to end, a reasonable period of notice (a minimum of one month) should be given and agreed to allow both parties time to consider and plan alternative arrangements.

To ensure the remote working arrangement is effective, an annual review will be conducted by the line manager to ensure the business needs are met and the arrangement is still efficient.

On an ongoing basis Remote Working agreements will be reviewed at least annually by the Faculty or Department to ensure the arrangement continues to meet any change in business demands. Remote Working agreements may also be reviewed as a result of any team or departmental changes.

5. Governance Requirements

5.1. Implementation: Communication Plan

The procedure was embedded when first published.

5.2. Implementation: Training Plan

The procedure was embedded when first published.

Further support will be provided to colleagues implementing the procedure when required.

5.3. Review

This procedure will be reviewed every 3 years or sooner if required by a change in legislation or practice.

5.4. Legislative Context and Higher Education Sector Guidance or Requirements

General Data Protection Regulation 2016/679

Data Protection Act 2018

5.5. Sustainability

SDG 11: Sustainable Cities and Communities. The accommodation of remote working will seek to reduce the environmental impact caused by commuting.

Home working reduces carbon emissions from both campus energy use as well as transport related to commuting. It does increase carbon emissions from staff own homes. These emissions may result in no overall change in carbon emissions.

Future studies should be undertaken to monitor home working carbon emissions to verify this balance of carbon emissions and to inform any remedial action that might be required to avoid a net gain in carbon emissions associated with the activity of the University.

6. Stakeholder Engagement and Equality Impact Assessment

An Equality Impact Assessment was completed on 10 December 2024 and is held by the Authorised Co-ordinator.

Stakeholder Consultation was completed, as follows:

Stakeholder	Nature of Engagement	Request EB Approval (Y/N)	Date	Name of Contact
Governance	Review of V1.0	N	January 2024	Andrea Langley
H&S	Review of V1.0	N	January 2024	Matt Purcell
Sustainability	Review of V1.0	N	January 2025	Martin Wiles
Our Data	Review of V1.0 for Our Data purposes	N	28 November 2024	Ewan Robson
Cyber Security	Review of V1.0 where cyber security is referenced	N	28 November 2024	Tom Brown
Procurement	Review of University Insurance Policy Excess V1.0	N	06 January 2025	Mark Illingworth