UNIVERSITY OF SUSSEX

General Counsel, Governance and Compliance

INSTITUTIONAL ACCESS POLICY

1. OVERVIEW AND PURPOSE

1.1 The University fundamentally respects the right to privacy of its staff and students when providing them with personal email addresses, IT accounts, and/or University-owned devices in order to facilitate their work and study at the institution.

1.2 However, the use of University systems and devices also carries with it responsibilities and obligations for individuals, as members of the University community and representatives of the institution, and the University also has a number of regulatory, compliance, and legal obligations that it is required to meet, as well as a need to ensure business continuity.

1.3 As such, there may be times when the University (or relevant third parties) may need to access the IT accounts, communications, devices, or stored data of individual users, and this may need to happen without the individual's consent.

1.4 The purpose of this policy is to provide clarity and transparency around when and why the University may require access to individuals' IT accounts, communications, data, and devices, to explain how this is authorised, and to provide information around the guidelines and expectations in place to ensure that access is appropriate.

2. SCOPE

2.1 This policy applies to the University IT accounts of individual users, along with any communications contained within them, as well as any other data users may have stored on University-owned servers and University-owned IT equipment, including any peripheral devices or hardware.

3. RESPONSIBILITIES

3.1 IT Staff / Other Staff Requiring Access Via IT

3.1.1 IT Services staff are authorised to access or monitor accounts, communications, files, or devices, or to provide relevant access to other staff members, where required, insofar as it is necessary in order to fulfil the purposes outlined in this policy.

3.1.2 Any staff member accessing another individual's accounts, communications, files, or devices for authorised reasons outlined in this policy must do so responsibly – i.e. they must ensure that confidentiality is maintained, that the information accessed is only for the specified purpose, and that any information that needs to be retained outside of the original user's account / email / device is safeguarded appropriately.

3.2 Chief Digital Transformation Officer

3.2.1 The Chief Digital Transformation Officer is responsible for providing authorisation to IT Services staff (or other relevant staff, via IT Services) to access individuals' accounts, communications, files, and devices for operational purposes.

3.3 General Counsel and Head of Information Management and Compliance

3.3.1 General Counsel and the Head of Information Management and Compliance are responsible for providing authorisation to IT Services staff (or other relevant staff, via IT Services) to access individuals' accounts, communications, files, and devices, where required to meet legal and compliance requirements.

3.4 Chief Operating Officer

3.4.1 The Chief Operating Officer is responsible for providing authorisation to IT Services staff (or other relevant staff, via IT Services) to access individuals' accounts, communications, files, and devices, where required in exceptional circumstances.

4. POLICY

4.1 Accessing Individuals' Accounts

4.1.1 The University will only access the IT accounts, communications, and data of individual users in specific circumstances:

- By request, or with the consent of the individual; or
- For operational purposes;
- To fulfil a legal or compliance obligation; or
- In other exceptional circumstances, for example, when there is a suspected breach of University regulation or policy or suspected criminal activity.

4.1.2 When access is required, and where it is appropriate and feasible to do so, consent will be sought.

4.2 Operational Reasons for Access

4.2.1 Access may be required for the following operational reasons, such as:

- To provide IT Helpdesk support and to ensure operational effectiveness of a service;
- To ensure that appropriate measures are taken with relation to cyber security threats (e.g. viruses, hacking, etc); or
- To access communications or files that are needed to carry out or ensure continuity of University business during periods of unexpected staff absence or following staff departure from the University.

4.3 Legal / Regulatory / Compliance Obligations

4.3.1 Access may be required in order to meet legal requirements or to fulfil regulatory and compliance obligations, for instance:

- To meet the University's obligations with regard to requests made under the Freedom of Information Act 2000;

- To comply with data protection legislation or take action following a personal data breach; or

- To carry out the University's statutory responsibilities under the Prevent Duty.

4.3.2 Access may also be required to provide information to third parties to meet other legal obligations, such as disclosure for law enforcement purposes or to comply with court orders.

4.4 Suspected Breaches of University Regulations or Policy

4.4.1 Access may also be required in other exceptional circumstances; for instance:

- When there has been a suspected breach of the University's Regulations (for example, a Student Discipline matter, academic misconduct, or expected misuse of the University's IT facilities); or

- When there has been a suspected breach of University policy or procedure (for example, research misconduct, expected misuse of the University's IT facilities).

4.4.2 Where a breach is suspected, investigation will need to be carried out in order to establish the existence of facts / evidence in order to invoke the appropriate disciplinary procedures where required.

4.4.3 Access may also be required where there is suspicion that University IT facilities are being used to commit or attempt to commit a criminal offence, in order to investigate and report to the police or other relevant authorities.

4.5 Misuse or Unauthorised Access

4.5.1 Where any individual is found to be accessing another person's University email communications, IT account, files stored on University servers, or University-owned devices for any reason other than the authorised reasons outlined in this policy, and/or where it is not required as part of their role at the University, they may be subject to disciplinary action.

5. LEGISLATION AND GOOD PRACTICE

5.1 The University's approach to institutional access, as laid out in this policy, is in accordance with rights and responsibilities in civil and criminal law (e.g. data protection legislation, the Freedom of Information Act 2000, the Human Rights Act 1998, the Employment Rights Act 1996, etc.)

5.2 Additionally, the University issues a number of its own regulations, policies, and procedures which outline expectations for appropriate and lawful use of its IT facilities; the key documents are linked below.

Review / Contacts / References	
Policy title:	Institutional Access Policy
Date approved:	23 May 2022
Approving body:	University Executive Group
Last review date:	N/A
Revision history:	New version created April 2022
Next review date:	May 2025
Related internal policies, procedures, guidance:	ITS Policies (including Regulations for Use of Information Technology) Data Protection Policy Information Classification and Handling Policy University Regulations
Policy owner:	General Counsel, Governance and Compliance
Lead contact / author:	Information Manager