

# University Computing Regulations

The University of Edinburgh has adopted a set of Regulations to cover the use of all its computing and network facilities by staff, students and any other persons authorised to use them.

## Regulations covering the use of Computing Facilities

23<sup>rd</sup> Edition August 2019

### Introduction and Definitions

These Regulations cover the use of all computing facilities administered on behalf of the University of Edinburgh (hereafter UoE). They will be reviewed periodically and amended as required. Amended Regulations will be published as a new edition; where no amendments are required, the current edition will be republished. The Regulations will be (re)published in August of each year.

As well as these Regulations, users must abide by other policies and/or codes as relevant, including but not limited to internal UoE codes such as:

- the [Code of Student Conduct](#);
- the [relevant staff disciplinary policy](#);
- the [University Data Protection Policy](#);
- the [Dignity and Respect Policy](#), [Trans Equality Policy](#) and any related documents;
- the [policy on taking sensitive information and personal data outside the secure computing environment](#);
- the [Information Security Policy](#);
- the [Bring your own device policy: Use of Personally Owned Devices for University Work](#).
- [the Protocol for Access to Data from the Corporate Student Record System](#)

And external codes such as:

- the Acceptable Use Policy of the Joint Academic Network (JANET) available on the Web at <https://community.jisc.ac.uk/library/acceptable-use-policy> (PDF);
- any terms of use or similar codes imposed by remote sites, where their computing facilities are accessed or used by UoE users; and
- any terms of use of similar codes imposed by any third party website or services accessed using UoE computing facilities.

It is not the intention of UoE that these Regulations should be used to unreasonably limit recognised academic freedoms.

## **In these Regulations**

"computing facilities" includes central [computing] services as provided by UoE Information Services Group and any [computing] service operated by or on behalf of UoE; UoE School or College or Professional Services; computers, IT hardware and services; personally owned computers and peripherals, and remote networks and services, when accessed from or via UoE computing facilities; and all programmable equipment; any associated software and data, including data created by persons other than users, and the networking elements which link computing facilities.

"users" include UoE staff, UoE students, and any other person authorised to use computing facilities

"files" include data and software accessed via the computing facilities (but do not include manual files).

## **Regulations**

### **1. Status of Regulations**

Breach of these Regulations by UoE staff or students is a disciplinary offence and may be dealt with under the appropriate disciplinary code or procedures. Where an offence has occurred, or is suspected to have occurred under UK or Scots law, the relevant user may also be reported to the police or other appropriate authority. The rules applicable to UoE's investigating of breaches or suspected breaches are in Regulation 6 below.

### **2. Private and inappropriate use of computing facilities**

Computing facilities are provided solely for use by staff in accordance with their normal duties of employment, and by students in connection with their university education. All other use, by any users is private. Private use is allowed, as a privilege and not a right, but if abused will be treated as a breach of these Regulations. Users should also note that, in the event of a breach of these Regulations, their personal information may be deleted by UoE in accordance with Regulation 6. Any use which does not breach any other Regulation herein, but nonetheless brings the University into disrepute, or breaches any other internal or external policies and/or codes with which a user is bound to comply from time to time, may also be treated as a breach of these Regulations.

### **3. Damage of computing facilities**

No person shall, unless appropriately authorised, take any action which damages, restricts, or undermines the performance, usability or accessibility of computing facilities; "taking action" may include deliberate omission or neglect, where action might reasonably have been expected as part of a user's duties.

#### 4. **Compliance with UK civil and criminal law**

Users must comply with the provisions of all current applicable UK or Scots law, including but not restricted to:

- a. intellectual property law, including laws concerning copyright, trademarks, and patents;
- b. the Computer Misuse Act 1990, and associated instruments;
- c. data protection laws; including the Data Protection Act (2018) and GDPR;
- d. Freedom of Information laws;
- e. the interception and monitoring laws under the Regulation of Investigatory Powers Act 2000 (RIPA 2000); and
- f. the Terrorism Act 2000, the Terrorism Act 2006 and the Counter-Terrorism and Security Act (2015)

Under the Lawful Business Regulations (LBR), the UoE draws to the attention of all users the fact that their communications may be intercepted where lawful under RIPA 2000. The full University notice can be found at URL

<http://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations/statutory-notices>

The UoE also draws to the attention of all users the University's statutory obligation under the Counter-Terrorism and Security Act (2015) and under the Prevent Duty to have due regard to the need to prevent people being drawn into terrorism. The full University notice can be found at URL

<http://www.ed.ac.uk/schools-departments/information-services/about/policies-and-regulations/statutory-notices>

The Terrorism Act (2000) defines terrorism in section 1 of the Act, see

<http://www.legislation.gov.uk/ukpga/2000/11/section/1>.

Users must also comply with the terms of any licence agreement or terms and conditions between the UoE and a third party which governs the use of hardware, software or access to data when such use or access is facilitated by the computing facilities.

If users are accessing a service via UoE computing facilities that is hosted in a foreign jurisdiction, they may also be subject to local laws which apply to that service. In these case, particular care should be taken to comply with any relevant terms applicable to that service.

#### 5. **Security, confidentiality and passwords**

Users must take all reasonable care to maintain the security of computing facilities and information to which they have been given approved access. In particular, users must not transfer or share their passwords, IT credentials or rights to access or use computing facilities, with anyone else. The confidentiality, integrity and security of all personally identifying data held, or processed on UoE systems must be respected, even where users have been

authorised to access it. Users must not attempt to obtain or use anyone else's credentials.

Users must ensure that portable devices used to access UoE information are protected by encryption, whether the device was purchased by the University, is personally owned or belongs to a third party.<sup>1</sup>

Guidance on how to encrypt portable devices can be found at <http://www.ed.ac.uk/infosec/how-to-protect/encrypting>

Prior to terminating their relationship with the UoE, users must make appropriate arrangements for the secure return of all UoE computer equipment and for the secure destruction of UoE data in their possession, unless alternative arrangements are agreed beforehand with their line manager and approved by Head of School/Support Unit

Users must ensure the secure destruction of all UoE data prior to disposing of computer equipment, including personally owned devices. These requirements also apply if any equipment is being sent for repair or upgrade as these actions could allow unauthorised third parties to access UoE information. If users are unsure of how to undertake this requirement, they must contact their IT support team for advice prior to disposal or repair of the computer equipment.

Passwords used to access UoE systems or data must not be used to access external services such as Facebook, personal emails etc. Additionally, where possible, the same limitation should apply to usernames used in the UoE, whether centrally generated or created by individual users.

## **6. Investigation of breaches**

If the UoE suspects any breach or potential breach of the Regulations by any user,, it shall have full and unrestricted power to access all relevant computing facilities and files (including mobile devices and privately owned devices used to access UoE services, including UoE email) and to take all steps which it may deem reasonable to remove or prevent distribution of any UoE material. It may also require that any encrypted data is made available in human-readable form. UoE may also immediately suspend a user's access to computing facilities and, where appropriate, examine such user's mobile device(s) for UoE material and remove any such material pending an investigation by an Authorised Officer or nominee of UoE as defined in the relevant Discipline Code where the user is a UoE staff member or student. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from UoE material in all circumstances. In particular, where a user's personal data is contained alongside UoE data (for

---

<sup>1</sup> Please note that iPhones and iPads are automatically encrypted if you set a password. Android has an easy option in settings to encrypt the device.

example, if a personal email is sent or received using UoE's email system), it will not be possible to distinguish this from UoE data and such personal data may be wiped. For this reason, you are encouraged not to use UoE email for personal purposes and, if you do, to mark any personal emails "personal" in the subject header. Users who use mobile devices for UoE related activity should also regularly backup any personal data contained on their device(s).

## 7. Liability

By using the computing facilities each user agrees that the UoE shall (to the maximum extent permitted by law) have no liability for:

- a. loss or corruption of any files or data contained therein;
- b. loss or damage (including any special, indirect or consequential loss) to users or to third parties, or their equipment, operating systems or other assets.

Each user agrees that UoE has the right to take legal action against individuals who cause it to suffer loss or damage (including damage to its reputation) as a result of that user's breach of these Regulations, and to seek reimbursement of such loss, and/or any associated costs (including the costs of legal proceedings) arising from such a breach.