The
University
Of
Sheffield.

University
Secretary's
Office

Guidance on the Use of Personal Electronic Devices and Email Accounts

March 2020

Authors: David Swinn, Head of Governance; Dr Tony Strike, University Secretary

1. Introduction

This guidance is intended to support lay members of Council and committees in making decisions about whether they wish to use a personal mobile device and/or email account for University business rather than the University account that is provided as a matter of course and/or any mobile device provided by the University.

This guidance has been prepared on the basis of legal advice from the University's Solicitors.

This guidance should be read alongside the University's Information Security Policy, and related procedures, Regulation XXIV: Use of Computing Facilities and the University's IT Code of Practice and supplementary Guidance.

Any member who elects to use their personal (or other non-University) device and/or email account for University business should comply with the requirements set out at Section 5, below.

Context

2. Practical advantages of using personal email accounts and devices

The University recognises that there are reasons why members may prefer to use alternative accounts (or devices) to conduct University-related business. These include:

- In some circumstances it may be inconvenient or impractical to use a University email account. For example, if members need access at their place of employment they may be prevented from doing so by local internet access restrictions.
- Using single email account means only having to remember one set of log in details.
- Using a personal (or other non-University provided) device avoids the need to use multiple devices for different purposes.

3. Practical disadvantages of using personal email accounts and personal devices

- Inefficiency:

  It is not possible to sync responses to electronic meeting and event invitations sent through Google Calendar meaning that direct follow-ups are needed to confirm acceptance. Members who have accepted may not be able to see in advance who else will be attending.

- Network Access difficulties and Delays:

  Members need to use their University log-in details to access eduroam. Once logged in, devices should automatically reconnect without the need to re-enter log-in details. In the event of connection problems and members being required to re-input their university log-in details, these may have been forgotten if they are rarely used. If members cannot access eduroam they would need to use mobile internet or guest Wi-Fi, which is less secure and can cause delays, particularly at meetings.

4. Legal Risks

Legal risks of using personal email accounts and/or personal devices to conduct University business include (and are set out in greater detail, below at paragraphs 4.1-4.3):

- Lack of information security.
- Unacceptable use of emails: the University could not control or, if required recover, any emails containing inappropriate or defamatory language about the institution.
- Increased difficulty discharging statutory data privacy obligations.
- Access: the risk of disclosure.

UK law imposes a number of other requirements on the use of IT, regardless of the email account or device used. In the context of members using personal devices in a University context, these are relevant to any communications sent over the University's Wif-Fi networks.

For example, it is unlawful to:

- Create or transmit, or cause the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- Create or transmit material with the intent to cause annoyance, inconvenience or needless anxiety;
- Create or transmit material with the intent to defraud;
- Create or transmit defamatory material;
- Create or transmit material such that this infringes the copyright of another person or organisation;
- Create or transmit unsolicited bulk or marke3ng material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their user organisation has chosen to subscribe;
- Deliberately (and without authorisa3on) access networked facilities or services.

4.1 Information Security

Personal email accounts and personal devices are likely to be subject to less stringent security controls than University accounts and devices. If University information is distributed externally, whether in error or maliciously, then the University would be unable to detect or trace this information.

Access to University networks and systems from personal devices increases the threat of exposure to cyber-security risks (e.g. malware) if that personal device is infected. Devices which are insufficiently secured are more vulnerable to attack/infection.

If a personal email account is compromised (i.e. "hacked") any information it contains could be accessed by unauthorised parties.

Physical loss or theft of a personal device could result in unauthorised access to university information and potentially to University systems.

4.2 Data Protection and Freedom of Information

Ultimate responsibility for compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) rests with the University, as data controller. The University is responsible for any personal data which members hold in relation to their University roles.

The University is responsible for implementing "appropriate technical and organisational measures" to protect personal data against misuse, loss or damage. Although the amount of personal data contained in correspondence and meeting papers is relatively limited, if the University is unable to readily access members' personal email accounts or personal devices it will be extremely difficult to ensure that any personal data held is protected by appropriate technical and organisational measures. It will also be more difficult to assess risks and apply any common measures across varying hardware.

The University may be obliged to report any breach of personal data to the Information Commissioner's Office (ICO) within 72 hours. Members must report any such breach (loss, theft etc) to the University promptly to ensure that the University complies with its statutory reporting obligations, thereby mitigating the risk of negative attendant publicity and regulatory sanction.

Information held in private email accounts may be subject to the Freedom of Information Act (FOIA) if it relates to official University business. Information held in personal accounts or devices will be harder to establish, making it more difficult for the University consider any such information in responding to an FOIA request. In the event of such a request, members must comply with request for information from the University in a timely manner. The same would apply to a Data Subject Access Request in relation to personal data.

In accordance with the data minimisation principle under the GDPR, once personal data is no longer required, it should be deleted.

4.3 Access

<u>Risk of disclosure of members' personal information</u>:

Using personal email accounts and/or devices blurs the delineation between University and other business, as the accounts and devices will include both types of information. In the event that the University or other agency, e.g. law enforcement, required access to University-related information then any personal information of the members could be inadvertently reviewed or disclosed.

5. Requirements for Using Personal Devices and Email Accounts

Any member who wishes to use or to continue to use personal (or other non-University) devices or email accounts should comply with the following:

- Comply with the University's Information Security Policy, and related procedures, Regulation XXIV: Use of Computing Facilities and the University's IT Code of Practice and supplementary Guidance.
- Dedicated folders should be used to hold University-related correspondence and other business.
- Protect of university information and personal data in accordance with sections 4.1 and 4.2, above, including compliance with the data minimisation principle.
- University information should not be stored on personal devices as far as possible. Where necessary, separate folders should be used for University business and information or data should be deleted as soon as it is no longer required. The vast majority of information provided to members would be available on request from the University Secretary's Office.
- Requirement to use a secure connection when accessing university information
- Comply with minimum security measures for each device: e.g. encryption, PIN numbers/passwords, virus protection, download controls.
- Immediately report any suspected or actual loss, theft or unauthorised access to personal email accounts or devices.
- Comply with any request from the University regarding FOIA requests or DSARs
- Comply with the general requirements of UK Law relating to IT.