University of Sheffield | University Secretary's Office

Policy and Guidance on the Use of Personal Electronic Devices and Email Accounts

December 2024

Authors: David Swinn, Head of Governance; Jeannette Strachan, University Secretary

1. Introduction

This guidance is intended to apply to lay members of University committees in conducting University business. It replaces previous guidance, developed in April 2020, in response to the increasing cyber and information security threats and related institutional and personal risks and developing sector practice in this area. This guidance also takes into account the latest institutional policies and guidance from IT Services, the University's use of Google suite, and the issues this can cause lay members, the planned introduction of a

new board portal solution. It also reflects earlier legal advice and discussions and comment through CUC and OfS in relation to lay members' use of personal email accounts (and devices) in relation to university business.

2. Relevant University Policies

2.1 (Staff) Code of Conduct

The section 'University processes, procedures and regulations' includes that everyone will "Ensure University information and data is kept confidential and secure. Visit our IT Services web pages for further information."

2.2 Information Security Policy

This Policy applies to all University information assets and/or information systems controlled by the University and to all areas of the University's business and the people and organisations involved in it. It includes the provision that anyone in scope of the policy will "Ensure that information and information systems under their control are protected appropriately and in line with information security policies and standards, seeking advice where necessary".

2.3 Information Classification and Handling Scheme

Under the scheme, all information in classes other than "Public" (i.e. Internal, Restricted and Highly Restricted) should only be accessed through a University account, unless by exception with express authorisation from the information owner/sponsor. Most of the information received by Council, and most other lay committee members, is at least Internal and more often than not Restricted.

2.4 Council Members Code of Conduct

The first point of the Code of Conduct states:

"I will recognise and understand that the Council is part of the constitutional and administrative structures of the University of Sheffield and act within the governing documents of the University of Sheffield and the law, and abide by the policies and procedures of the organisation. This includes having a knowledge of the contents of the Charter, Statute, Regulations and Standing Orders of the University and relevant policies and procedures, all of which is covered upon induction."

3. The Approach

The University strongly encourages all lay members to use their University email and IT account in their University business and will limit the amount of information sent directly to non-University accounts. Multi-Factor Authentication/Single Sign-On (MFA/SSO) will be implemented for all lay members' University accounts in line with other University IT accounts and general good practice.

3.1 Email and IT accounts

Only University accounts must be used to access meeting papers and other University-related information or documents, including via Google Drive and through the new board portal, enabling the use of University MFA or SSO. No detailed information, including meeting papers, offline approvals or other University business-related information will be sent directly to non-University accounts.

Where members indicate a preference for doing so, basic notifications may be sent to non-University accounts to advise that correspondence or other information requiring their attention has been sent to their University address.

3.2 Devices

Lay members are not required to use a University-provided device, due to the costs to the University and added inconvenience to users, provided that any personal device meets the University's IT policy requirements for security and/or encryption. Personal devices can be set up so that members can use their University IT account as well as any personal or work accounts that they may have. The University will provide a device to any member who does not have their own device to use.

Dedicated support and guidance is available to all members as part of their induction and on an ongoing basis to ensure that they can access and use their University accounts and that their device is set up correctly.

4. Any member using a personal device

In line with institutional policies and practice, any member who wishes to use or to continue to use personal (or other non- University) devices should comply with the following:

- Comply with the relevant University policies referred to under section 2 and related procedures, Regulation XXIII: Use of IT Facilities and the University's IT Code of Practice.
- Dedicated folders should be used to hold University-related correspondence and other business.
- Protect of university information and personal data in accordance with section, 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, where they contain or may contain University information.
- Comply with any request from the University regarding FOIA requests or DSARs.
- Comply with the general requirements of UK Law relating to IT.

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

5.1 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.

5.2 Network Access Difficulties and Delays

Members need to use their University login 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 login 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.

6. 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 6.1-6.3):

- 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 marketing 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 authorisation) access networked facilities or services.

6.1 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

6.2 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 to consider any such information in responding to an FOIA request. In the event of such a request, members must comply with requests 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.

6.3 Access: Risk of disclosure of members' personal information

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.