EMAIL MANAGEMENT POLICY STATEMENT

1) Introduction

As with other Information and Communications Technology (ICT) facilities, email services are provided to staff by Edinburgh Napier University for educational purposes and conducting University business and research. Email is one of the preferred methods of corresponding for business purposes and its vulnerability when outside the University's secure electronic network and ease of distribution and proliferation increase the risks inherent in its use. This policy aims to ensure that**:** email users are aware of their responsibilities**;** both individuals and the University are protected**;** and**,** that the effectiveness of email as a business tool is maximised.

2) Purpose

The purpose of this policy statement is to ensure that all employees of the University are aware of the obligations placed on the University and its employees by legislation governing electronic information and communications, and that emails and the email system are used appropriately, effectively and responsibly as per the relevant guidance.

This Policy Statement deals with email management in two (2) parts as follows:

- **Legislation and best practice (s.5 below)**: emails *sent* from University accounts constitute formal business communications/ correspondence which are subject to scrutiny under various pieces of legislation. Breaches of legislation most commonly occur through**:** user error**;** lack of awareness of legislation and policy requirements**;** complaisance**;** and**,** abuse of the system – raising awareness of the issues helps to reduce risk and protect individuals against inadvertently breaching legislation and/or policy.
- **Email records and email account management (s.6 below)**: email accounts provided by the University must be managed appropriately to ensure that the security and availability of University information and records is maintained, along with efficient operation of the email system.
  The University email system is a communication tool NOT a filing system.

3) Scope

This Policy Statement applies to all employees (including short-term or casual and student employees), associates and contractors employed by the University who have been allocated a University email account to their individual network login, and also encompasses employees who manage or access generic (public or shared) team/ departmental email accounts ("users").

This Policy Statement covers all information and University records communicated and/or held in email format, including attachments and embedded data.

4) Policy Statement

The University requires users to:

- Comply with the legislation and best practice recommendations,
- Use the email facilities provided responsibly and appropriately,
- Actively manage the email mailboxes for which they are responsible to ensure efficient use of resources,
- Ensure University records held in email format are managed appropriately.

The University is committed to:

- Compliance with the legislation,
- Ensuring all employees are aware of their responsibilities and the consequences of non-compliance with this policy statement,
- Providing advice and guidance resources to promote user compliance.

The University reserves the right to include disclaimers as necessary in all email communications.

5) Legislation, and Best Practice

The applicable legislation is listed below along with a brief outline of the main relevant notes which include best practice guidelines where necessary:

Computer Misuse Act 1990

This Act makes it an offence to:

- Maliciously corrupt or erase data or programs e.g. download from a received email or send an email containing viruses or malicious software;
- Make unauthorised use of computer facilities or unreasonably waste computer resources and time.

Data Protection Act 2018 and General Data Protection Regulation 2016

- Users sending personal data externally by email must encrypt or password protect the information. Guidance can be found in the University's DP Code of Practice, encryption advice and email guidance and Information Security Classification Scheme
- Individuals are entitled to request a copy of any information held about them e.g. their personal data - this includes information in email format. It is an offence to alter or destroy that information once it has been requested by an individual. Care should be taken not to include inappropriate comments in emails which may be disclosed in response to an access request.

Privacy and Electronic Communications Regulations 2003 (PECR)

- Consent by affirmative action must be collected from individuals before they can be sent any communications designed to influence or change recipients' behaviour. Consent must be as easy to withdraw as to give and records of consent must be maintained. Opt-out tick boxes are *not* allowed (opt-in boxes/options are required).
- Any approved email marketing activities must adhere to the University PECR guidance.
- Sending unauthorised, unsolicited marketing material, chain letters and 'junk' mail of any kind from University email accounts is prohibited.
- Members of staff should not grant another individual access to their email account unless exceptional circumstances apply and it is authorised by a senior manager.

Freedom of Information (Scotland) Act 2002 (FOISA)

- To ensure that information is available for FOISA responses and enable the University to observe the Scottish Ministers' Code of Practice on Records Management as required under s.61 of the Act, please see section 6 below.
- University business should not be conducted by employees through non-University email accounts – any such communications are subject to FOISA.

Regulation of Investigatory Powers Act (Scotland) 2000

- The University conducts authorised monitoring as detailed in the University Monitoring and Logging Policy (Electronic Information Security Policy) and the University's Privacy Notices.

Copyright, Designs and Patents Act 1988

- It an offence to use or copy all or part of any work/s which are protected under the legislation, without permission or acknowledgement, including sending by email.
- The University has a comprehensive copyright guidance resource available online.

Communications Act 2003

- It is an offence to send a message or other content that is grossly offensive or of an indecent, obscene or menacing nature or where the sender's address is masked or 'anonymous'. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Please note that this list is not exhaustive and there is additional applicable legislation; please see the University Email Guidance for more information.

6) Email records and email account management

The predominance of business being conducted by email means an increase of official University records being held in this medium which must be managed in accordance with the Records Management Policy. It is important that email records are stored in shared network areas which are accessible to appropriate colleagues and have the necessary security controls in place. The importance of this practice is highlighted when colleagues are absent/leave the University, requests under "Access to Information" legislation are received or email records documenting contract negotiations and agreements are required as evidence.

Email accounts must be continuously maintained to ensure messages with no continuing value are deleted and those which constitute records are retained as above, to ensure efficient operation and effective use of the system.

Comprehensive guidance is available from Governance Services and Information Services.

7) Responsibilities

All Email Users: *All* users are responsible for ensuring that all emails sent and/or managed by themselves on behalf of the University are done so in compliance with legislative and University policy requirements including the Information Security Policies, Records Management Policies and Data Protection Policy Statement and Code of Practice.

If you require to send an all staff email please contact the Engagement and Communications Consultants in Human Resources to discuss your request.

Staff with all staff email access: Staff who have access to send out mass/bulk emails to all staff must ensure they inform the Engagement and Communications Consultants before issuing an all staff email. The only exceptions are staff who are named in the University's crisis communications plan.

Personal use is covered in s.6 of the Information Security User Policy and specifically excludes use for any form of personal financial gain, competitive business or where a conflict of interest may arise.

Managers: All managers are responsible for ensuring that this policy and any associated procedures are implemented in their service area. They should ensure team members have read and agreed to abide by the policy and are aware of their responsibilities in this regard, and receive any additional training required.

Managers must ensure an appropriate mass email distribution (e.g. All Staff) procedure is implemented in their area detailing responsibilities and authorisation. Any misuse of bulk email will be dealt with by the relevant member of Senior Leadership Group.

Information Services (IS): will provide email facilities and systems, and associated system guidance and training. As these systems are provided for business purposes IS have procedures for accessing individuals' University email account for the purpose of recovering business information or information relevant to any criminal investigation.

Governance Services: will provide information governance advice, training and guidance.

The University Secretary: has overall responsibility for ensuring the University complies with information legislation.

8) Sanctions for Non-Compliance

The Electronic Information Security Policy s.9.0 refers: Failure of a user to comply will lead to the relevant disciplinary procedures being invoked and further legal action may be taken.

9) Policy Contact/Resources

Queries about this Policy can be directed to:
Governance Services - https://staff.napier.ac.uk/services/governance-compliance/Pages/who.aspx

As this document contains multiple hyperlinks readers are advised to access it, and the accompanying comprehensive guidance, online at:
https://staff.napier.ac.uk/services/governance-compliance/governance/records/email/Pages/default.aspx

10) Document Control Information	
Title (Full name of current version: title, version number, status)	Email_Management_Policy_Statement_V2.1_CURRENT
Document type	Policy Statement
Date approved	28/11/2017
Approved by	University Secretary on behalf of ULT
Responsible manager	Diana Watt
Review frequency	Biennially
Next review date	October 2019
Scope	All University employees/agents using email facilities (“users”)

Document Review Table				
Date	**Action by**	**Version updated**	**New version number**	**Brief description of update**
20150723	DW/Governance		V0.1	First version
20150919	Governance	V0.1-V0.4	V0.5	Various internal drafts/updates
20150924	UIGG		V1.0	Consultation
20170615	AP/HR	V0.1	V0.2	HR Internal Communications Adviser inclusions
20170615	DT/IS	V0.2	V0.3	Information Services inclusions
20171128	GW/ULT	V0.3	V2.0	Approved
20190619	DW 20190619	V2.0	V2.1	Minor updates, legislation references and links