AGENDA ITEM NO 9

REPORT NO 193/21

ANGUS COUNCIL

POLICY & RESOURCES COMMITEE – 8 JUNE 2021

APPROVAL OF EMAIL USAGE POLICY

REPORT BY SHARON FAULKNER, DIRECTOR OF HR, DIGITAL ENABLEMENT, IT & BUSINESS SUPPORT

ABSTRACT

This report presents and seeks approval for the new email usage policy.

1. RECOMMENDATION(S)

It is recommended that the Committee:

(i) notes the inclusion of elected members element in the new email usage policy with the implication that it equally applies to elected members and employees;

(ii) reviews and approves the email usage policy attached as Appendix 1

2. ALIGNMENT TO THE COUNCIL PLAN

2.1 This report supports the council's aim to be efficient and effective by ensuring that our email facilities are used effectively and for their intended purpose.

3. BACKGROUND

3.1 The continuing use, and availability, of information systems is essential to the operation of Angus Council and the use of email is a key component in this. For this reason, information systems, including email, must be recognised as major council assets and be protected accordingly. Protecting these information systems and setting out acceptable use of email is the purpose of this updated Email Usage Policy.

3.2 This policy is designed to safeguard both Angus Council and all users of its e-mail facilities. It aims to ensure that these facilities are used effectively, for their intended purposes and without infringing legal requirements or creating unnecessary business risk. The policy sets out general principles and specific rules. Its aims are to:

- promote the effective use of email facilities;
- ensure that all users understand what is permitted and what is not permitted when using email facilities;
- protect both the council and individuals from the possibility of legal action;
- protect the council's information technology systems from damage.

The summary messages of this policy are:

- emails and the email system are vital council assets and they need protected accordingly;
- council email must not be used for personal purposes;
- everyone needs to be alert to scam emails and make sure they are aware of what to do if they get one.

4. FINANCIAL IMPLICATIONS

4.1 There are no financial implications arising directly from this report.

5. EQUALITY IMPACT ASSESSMENT

5.1 An equality impact assessment is not required.

6. CONSULTATION (IF APPLICABLE)

6.1 Consultation has taken place with the Information Governance Steering Group, the Council's Leadership Team and recognised trade unions.

NOTE: No background papers, as detailed by Section 50D of the Local Government (Scotland) Act 1973 (other than any containing confidential or exempt information) were relied on to a material extent in preparing the above report.

REPORT AUTHOR: Caroline Cooper, Service Leader, Digital Enablement & IT
EMAIL DETAILS:IT@angus.gov.uk

List of Appendices:

1. Email Usage Policy v2.2

ANGUS COUNCIL

EMAIL USAGE POLICY

Version:	V2.2
Author(s):	Frank Hutcheon, Team Leader Network and Security
Date of Approval:	May 2021
Approved by:	IGSG
Date issued:	
Next review date:	May2022

Document Control Sheet

Author(s): Frank Hutcheon, Team Leader Network and Security

Document Title: Angus Council Email Usage Policy

Review/Approval History
Note previous published versions March 2005
Unapproved previous version of email policy circulated Dec 2018

Date	**Name**	**Position**	**Version Approved**	**Date Approved**
August 2019	Frank Hutcheon	Team Leader Network and Security	V1.0	
December 2020	Frank Hutcheon	Team Leader Network and Security	V2.0	

Version	**Date**	**Brief Summary of Changes**	**Author**
2.1	03/08/2020	Major change, employees, elected members and authorised agents (all users) should not be using council email address for private business.	Frank Hutcheon
2.2	16/12/2020	Incorporation of Summary and other changes from IGSG	Frank Hutcheon

Table of Contents

Email Usage Policy

The continuing use, and availability, of information systems is essential to the operation of Angus Council and the use of email is a key component in this.

For this reason, information systems – including email - must be recognised as a major council asset and be protected accordingly. Protecting these information systems and setting out acceptable use of email is the purpose of this Email Usage Policy.

Council information systems are used to enter, process, store, generate, or disseminate information and must be protected from misuse, unauthorised modification, damage, or disclosure by individuals internal or external to the organisation.

By selecting and implementing the appropriate controls, identified risk can be reduced to an acceptable level. These controls are selected considering the need to preserve the confidentiality, integrity and availability of the information and systems. Non-monetary factors, such as loss of reputation are also accounted for in this policy.

Operational procedures must be established to implement the corporate IT security requirements outlined in this Email Usage Policy, and appropriate mechanisms put in place to monitor and manage these procedures.

This policy is designed to safeguard both Angus Council and all users of its e-mail facilities. It aims to ensure that these facilities are used effectively, for their intended purposes and without infringing legal requirements or creating unnecessary business risk. The policy sets out general principles and specific rules.

Its aims are to:

- Promote the effective use of email facilities.
- Ensure that all users understand what is permitted and what is not permitted when using email facilities.
- Protect both the council and individuals from the possibility of legal action.
- Protect the council's information technology systems from damage.

The summary messages of this policy are:

- Emails and the email system are vital council assets – protect them accordingly.
- Do not use council email for personal purposes.
- Be alert to scam emails and make sure you are aware of what to do if you get one.

Scope

This Policy applies to all users of Angus Council's facilities or equipment. All users, include employees, temporary employees, elected members, employees from public and private sector partners and, contractors (hereinafter referred to as "authorised agents", wherever located. This scope also includes teaching staff who are employed by Angus Council and use the Angus Council corporate email system. It does not however include the use of Glow email provided to staff.

This policy does not apply to school pupils for whom there is a separate policy.

In addition, the use of Angus Council email facilities delivered to personally owned devices is included in this policy.

Related Documentation

The following Council documentation supports and reinforces the Angus Council Email Usage Policy:

Information Security Policy

Information Security User Guidelines

Password Policy and Guidelines

Data Protection Act 2018

Computer Misuse Act 1990

Note: ***Password Policy and Guidelines and Information Security User Guidelines will be updated in 2021.***

General Guidelines

All council IT resources, including email facilities, are provided primarily for business purposes, and for carrying out activities consistent with employee job outlines.

Employees, elected members and authorised agents must use the council's e-mail facilities responsibly, lawfully and in accordance with the terms of this policy and not in any way that might conflict with the council's interests.

When using Angus Council provided email facilities employees, elected members and authorised agents must not engage in any activity which is illegal, distasteful, offensive or likely to have negative repercussions for the council.

If you suspect any abuse or misuse of the email facilities you must report it to a manager immediately.

Breaches of the Policy

Employees who do not follow the terms of this policy may be liable to disciplinary action under formal established disciplinary proceedings and, depending on the nature of the breach, may also be liable to legal proceedings.

Non-employee users, e.g. Elected Members or authorised agents who breach the policy may have their access to the email facilities withdrawn and, depending on the nature of the breach, may be liable to legal proceedings.

Personal Use

The council provides email facilities to help employees, elected members and authorised agents carry out their role.

These email facilities must be used for council business purposes only.

Publicising your council email addresses for personal use is not permitted. This can assist cyber criminals and those with malicious intent in identifying legitimate addresses and can increase the burden on the council’s email infrastructure and security systems.

As a council employee, elected member or authorised agent you should not use your corporate email address to:

- Register for personal transactions
- Register with non-work-related websites (holidays, social media etc.)
- Be used as a contact address for non-work-related publicity.

Monitoring

The council continuously monitors the use of its e-mail facilities.

It does this to:

- Check service standards
- Help maintain the effective operation of information technology systems
- Help maintain the security and confidentiality of these systems
- Identify breaches of this policy
- Identify un-authorised, improper or criminal use of these facilities

To achieve these purposes the council monitors:

- Email traffic (volumes and patterns of usage)
- Message subjects
- Senders and recipients
- Size and type of file attachments
- The location council email is being sent and received to and from
- The device council email is being accessed on

Email is still the most widely used and successful attack method employed by threat actors when attempting to distribute malicious software and gain access to files and systems. To that end the council also employs an email security solution which scans all incoming and outgoing mail.

This solution removes:

- Known spam messages
- Virus infections
- Potentially harmful attachments
- Unsuitable content

While monitoring of all e-mail activity is possible this will not be done routinely unless illegal activity and/or breaches of this policy are suspected.
To ensure that information assets receive an appropriate level of protection, security classifications will be used to indicate the need and priority.

Business Use and Accessing Email

Angus Council will restrict access to the email systems to only those employees, elected members and authorised agents of the council who require such access to enable them to undertake their duties.

It is the responsibility of all Service Leads, and the Service Leader, Digital Enablement and IT to publicise and implement this policy as required and the responsibility of all employees, elected members and authorised agents to read and abide by this policy.

All users must only use the council's email system account for receiving work related email. Personal email accounts must not be used to send and receive work email and failure to comply with this may result in disciplinary action against the user.

Council employees, elected members and authorised agents should also bear in mind that an email can be as contractually binding as any other form of communication.

Inappropriate use of council email is prohibited. Some examples of this would be:

- Engaging in illegal activities.
- Encrypting personal emails and attachments.

Allowing other people to access their emails (unless authorised for work related purposes, such as, allowing a manager or a manager authorised colleague to access your email when for example on long term absence or departmental shared mailboxes.) Allowing a colleague to access your email for convenience is not acceptable.

Employees must only use the following equipment and methods to access their council email:

- Corporately provided equipment and software (desktop/laptop/Citrix)
- Corporately provided mobile devices (phones / tablets)
- Personal mobile devices configured with the council's mobile device management (MDM) software and the user agrees to the council's terms of use.
- Personal computing devices (PCs/laptops) – where authorised – may be used to access email via the council's Citrix environment.

Management and security of personal mobile devices to provide email access is a significant management overhead for the council IT service and there may be times when the IT service is no longer able to support a specific type of device. This may be for the following reasons:

- Security reasons – a device is unable to be patched to a required security level.
- The operating system of the mobile device is no longer supported by the device manufacturer.
- The MDM platform is no longer able to support a specific device model.

To that end the council reserves the right to disable access to email from personal devices which are no longer supported for the reasons above. This would generally be advised to the user in advance but there may be occasions where, for critical security reasons, the email on the device needs to be disabled without warning.

Any piece of council IT equipment used to access email and authorised for use out-with council premises, including but not restricted to laptop computers, phones and tablet devices, will be subject to the same guidelines for use as IT equipment within the workplace.

There should be no distinction made in relation to both the physical security of the council IT equipment used to access email and the security of your email account. Whether it is fixed (PCs etc.) or portable (laptops / tablets / phones) the same considerations must be applied. Whilst off-site or in transit, such equipment must be protected by the user from the risk of theft and must not be left unattended in public places.

Responding to Email Incidents

All council employees, elected members and authorised agents have a responsibility to report suspected breaches of this Email Usage Policy to their own service management who will in turn ensure that any security incidents will be recorded via the IT service desk by means of a formal logging and follow-up process.

Unless authorised by the Service Leader, Digital Enablement and IT, employees, elected members and authorised agents will on no account attempt to replicate or simulate any suspected email security breach or incident such as forwarding suspected email spam or malware.

Council employees suspected of being in breach of the council's Email Usage Policy will be subject to investigation under established formal disciplinary procedures.

If an elected member breaches this policy and procedures are not followed, then use of the council's facilities may be curtailed or withdrawn. Serious breaches of this policy may amount to a breach of the Councillors Code of Conduct and the withdrawal of permission to use the council's equipment and email services.

Sending and Receiving Secure Email

By default, all Angus Council email which is sent from an Angus Council email account is encrypted using TLS email encryption with the caveat that the receiving party must also support the TLS email encryption protocol on their receiving email server.

The majority of public sector organisations the council works with already support this protocol however the IT service does not maintain a record of who does and doesn't support TLS and it is the responsibility of the sender to ensure that when email requires to be encrypted that the receiving organisation supports TLS encryption.

In the event there is doubt there are other ways to send secure email/ attachments to third parties and details of this are provided in the Service Catalogue.

Email Backup and Retention

Council email back up facilities will be provided to ensure that all essential business information contained in email can be backed up and recovered if necessary.

Full details of the backup and restore service which includes email can be found in the Service Catalogue

Email is retained for 12 months in the user's personal mailbox.

Faults and Issues with Email

Faults in relation to the council email systems will be reported to the council's IT service desk where they will be processed in accordance with the Service desk procedures.

Only qualified persons authorised by the Service Leader, Digital Enablement and IT will carry out repairs and maintenance of the council's email system and client devices used to access the email system.

Management and Maintenance of Email Systems

The installation and upgrade of operational systems will only be performed by arrangement with the Service Leader, Digital Enablement and IT in accordance with the established Digital Enablement and IT change management processes.

Compliance

The council's Leadership Team will implement appropriate procedures to ensure that all procurement of email systems conforms to appropriate legislative requirements in addition to the council's Standing Orders and Financial Regulations.

System owners shall ensure that important council records potentially held in email systems will be protected from loss, destruction and falsification. Some records may need to be securely retained to meet statutory or regulatory requirements as well as to support essential business activities.

Note: ***System owners are the responsible person within a service which has responsibility for security of data held in that system and which may hold emails as part of any data collection.***

The Digital Enablement and IT service will ensure that all requirements in relation to the patching of hardware and software used to deliver the email service are implemented to ensure that compliance with the various codes of connection the council must adhere to are met.