Email, Internet & Acceptable Usage Policy

Ilfracombe Town Council

1 Introduction

1.1 Ilfracombe Town Council (the Council), provides email, internet access and access to IT facilities (via North Devon Council) to help support the Council's business requirements in an efficient and effective manner.

1.2 At points throughout this policy, there is reference to "*Council Business Use*" and "*Personal Use*". In essence, Council Business Use is any use that is carried out to support the genuine business operations of the Council – all other use is regarded as *Personal Use*.

2 Scope

2.1 This policy applies to all employees, elected Members and any individual or partnership organisation (hereafter referred to as Users).

2.2 This policy refers to "line manager", which should be taken to mean the line manager with the appropriate authority to make the decision.

2.3 The Council's email and Internet systems are primarily for Council Business Use.

2.4 Due diligence and care must be always be taken when considering the content of emails.

2.5 Users are responsible for ensuring that they use the internet facility in an effective, lawful and ethical manner, with respect for the privacy and rights of other individuals.

3 Breaches of this policy

3.1 Line managers are responsible for ensuring that their staff are made aware of this policy and that they attend appropriate training as deemed by the Council.

3.2 Failure to comply with this policy by staff of the council may result in disciplinary action being taken. Failure to comply by Members of the Council may constitute a breach of the Members' Code of Conduct.

3.3 In respect of para 3.2 the following are **prohibited** activities:

3.3.1 Masquerading as another user for the purpose of sending emails or accessing the internet.

3.3.2 Reading, deleting, copying or modifying the contents of another person's email mailbox without consent or other appropriate authority

3.3.3 Sending or forwarding emails with inappropriate content, for example pornographic, offensive, insulting, bullying, racist, obscene or threatening e-mail.

3.3.4 Sending chain letters or emails which encourage Users to send them onto other Users for non-business purposes.

3.3.5 Deliberately making comments in an email or on the internet that could damage the reputation of the Council or reasonably be used against the Council in litigation.

3.3.6 Posting offensive, insulting, bullying, racist, obscene or threatening information anywhere on the internet.

3.3.7 Using files downloaded from the internet in direct violation of licensing and/or copyright laws.

3.3.8 Accessing or attempting to access pornographic and other restricted sites, including those categorised as 'adult content', racist, threatening, anti-social, child pornography or promoting terrorist activities.

The above must not be considered an exhaustive list. If in any doubt as to permitted email content you should contact the ICT service desk in the first instance.

4 Monitoring of email & internet

4.1 External emails both sent and received are logged.

4.2 The Council reserves the right to inspect any emails or internet access at any time (particularly during investigations), where there is suspected email or internet misuse.

4.3 Users should be made aware that the Council will not attempt to differentiate council business use from personal use, and therefore all email use will be subject to the same inspection and retention.

4.4 Accidental breach of this policy must be reported immediately to the respective line manager who will contact the ICT Service Desk.

4.5 The use of the internet is recorded and the Council reserve the right to monitor all internet activity. **It is possible to identify internet sites visited by individual users.**

4.6 The ICT service, will regularly undertake monitoring of internet activity.

4.7 The Council will block access to certain internet sites as directed by Senior Management Team.

4.8 Secure web pages (usually denoted by a web address starting https:\\) will be monitored. Users should be made aware that confidential and personal files and information will pass through the monitoring system and details may be intercepted.

4.9 The Town Clerk may request internet usage reports from the ICT service. The Monitoring Officer may request internet usage reports for Members from the ICT service.

4.10 If users find themselves connected accidentally to inappropriate internet sites they must disconnect from that site immediately. Such unintentional access to inappropriate internet sites must be reported immediately to the ICT service Desk and contact their line manager.

5 Emails as records and business process

5.1 Emails have increasingly become more than an ad-hoc communication mechanism and are now use in place of paper records in many cases. Email has also become key to many Council business processes.

5.2 **It is the responsibility of the user to ensure that the recipients of an email are entitled to receive the email.**

5.3 Email messages and attachments are considered to be the Council's records and as such may be disclosable, or otherwise subject to individuals' rights, pursuant to the General Data Protection Regulation and/or the Freedom of Information Act 2000/Environmental Information regulations 2004.

5.4 Users are responsible for ensuring that all email accounts under their control are operated in accordance with this policy.

6 Computer viruses and malicious programs and material

6.1 Computers can be infected by viruses and malicious programs received via email. This could have a serious impact on the Council.

6.2 All emails will be scanned for viruses, known as malicious content, and known for high risk content types. Suitable filtering will be applied to manage this risk.

6.3 The Council runs anti-virus software. Users must contact the ICT Service Desk if any warnings regarding viruses are displayed on their desktop.

7 Secure Email

7.1 Emails sent between northdevon.gov.uk addresses are held within the same network and are unlikely to be illegally accessed. Messages sent outside these networks travel over the public internet and are exposed to the potential of being intercepted and read by anyone other than the intended recipient.

7.2 Files containing restricted information as defined in paragraph 13 of this policy, or containing personal information about an individual, must never be transferred using email without encryption. If there is a business need for suck information to be transferred using email, the ICT Service Desk must be consulted to ensure that an approved process is followed.

8 Unauthorised email access by ICT staff

8.1 All ICT staff are subject to this policy and its requirements. Unless previously authorised, ICT staff are not allowed to read the content of the mailboxes of other users. Should emergency access be required to a mailbox or ICT assistance be required as part of an investigation, then this must be authorised by the Line Manager.

9 IT Acceptable Usage

9.1 Computer software & equipment **must** only be installed or configured by ICT

9.2 The unauthorised loading or copying of software including copyrighted audio and visual software e.g. CDs and DVDs (or copying of associated copyrighted documentation) is prohibited as it is an offence under the Copyright, Designs and Patents Act 1988. All bona fide software and licences need to be held by ICT Services.

9.3 Unapproved software **must not** be loaded onto the Council's computers, under any circumstances. Where unapproved software is deemed to be of use to the Council then a request for approval must be raised with the ICT Service Desk.

9.4 ICT Services are authorised to remove software that is not required to fulfil the employee's duties.

9.5 Users must not attempt to access hardware, software or data for which they have no approval. Where a change is required in order to allow a user to fulfil their approved duties then a request for change must be raised with the ICT service desk.

9.6 All surplus equipment should be returned to ICT Services for disposal or storage.

9.7 All shared portable Council ICT equipment must only be removed from Council premises if either it has been booked out through the service area to which the equipment has been allocated for shared use, or it has been booked out through the ICT Service Desk.

9.8 The safekeeping of any equipment removed from Council premises is the responsibility of the person in control of the equipment, ensuring compliance with the Council's Insurance Policy which states "any equipment removed from the Council's premises must be taken into the home of the person who is in control of that item for overnight security". When in transit and for any short time the vehicle is left unattended, the item remains safely out of sight, i.e.: in the boot.

10 Information Security Incident Reporting

10.1 An information security incident occurs when data or information is transferred or is at risk of being transferred to somebody who is not entitled to receive it, or data is at risk from corruption. Such incidents may be accidental or deliberate.

10.2 An information Security Incident includes:

- The loss or theft of data, information or equipment
- The transfer of data or information to those who are not entitled to receive that information
- Attempts (either failed or successful) to gain unauthorised access to data, information storage or a computer system
- Computer infected by a virus
- Disclosure of a password
- Sending an email containing sensitive information to 'all staff' by mistake

The above should not be considered an exhaustive list. If in any doubt as to potential security incidents, you should contact the ICT Service Desk in the first instance and, where there has been a suspected loss of, or unauthorised access to, personal data, you must also

contact the Data Protection Officer or Information Commissioner's Office as a matter of urgency.

10.3 All Information Security Incidents must be reported initially to the immediate line manager who must then notify the ICT Service Desk. **Failure to report security incidents is a breach of this policy.**

10.4 The ICT Service Desk will create a security incident log and invoke the relevant procedures.

11 Viruses

11.1 All PCs (including laptops, notebooks and any other such equipment) are protected by virus detection software. Any suspected viruses should be reported immediately to the ICT Service Desk and should not be forwarded or deleted without their permission.

12 Removable Media

12.1 Due diligence and care must be taken over what data or information is transferred onto removable media.

12.2 Data on personal memory sticks can only be accessed 'read only' by the user.

12.3 NDC data held on the network can only be written to an encrypted memory stick supplied by the ICT Service Desk.

12.4 Whilst in transit or storage the data must be given appropriate security according to the type of data and sensitivity.

13 Information Classification

The Council will have two classifications of information, **Restricted** and **Unclassified**.

It is the responsibility of Line Managers to ensure all staff in their service are made aware of the definitions of restricted and Unclassified as defined below, and it will be their responsibility to make decisions on classifications of information within their service.

Restricted

Compromise of Restricted information would be likely to:

- Cause substantial distress to individuals
- Cause financial loss or loss of earnings potential to, or facilitate improper gain or advantage for, individuals or companies
- Prejudice the investigation or facilitate the commission of crime
- Breach proper undertakings to maintain the confidence of information provided by third parties
- Undermine the proper management of the public sector and its operations
- Breach statutory restrictions on the disclosure of information
- Disadvantage Government in commercial or policy negotiations with others

Unclassified

Compromise of Unclassified information would be likely to:

- Cause minimal inconvenience to any party
- No risk to any party's personal safety
- Minimal financial loss to any party
- No damage caused to any party's standing or reputation
- No distress caused to any party

13.1 Information will only be communicated through the methods that are appropriate to the information classification. A higher security requirement shall not be communicated through a lower communication method.

Restricted information may only be communicated by the following methods:

- Special delivery mail to an individual marked 'Addressee Only' with a return address on the envelope and sealed with tape
- Gcsx (local government), gsi (Central Government), pnn (police), providing both email addresses are one of these, secure fax, registered post, sealed envelope in internal courier
- Do not allow third parties to overhear conversations
- Must not be made available on a public web site. HTTPS to be used for internet transfer
- Handle, us and transmit with care, take basic precautions against compromise or opportunist attack

Unclassified information may be communicated in the following ways:

- Unsecured Internet email, fax, courier, ordinary post, telephone

13.2 Information will be disposed of as below

Restricted:

Dispose of sensibly by destroying in a manner to make reconstruction unlikely. Use a shredder or put documents in a confidential waste bin that is collected by an approved contractor

Unclassified:

Use recycling facilities

Policy reviewed: 14/2/22
Adopted: 09/9/19
Next review: 14/2/24