LISKEARD TOWN COUNCIL

INFORMATION TECHNOLOGY USAGE & SECURITY POLICY FOR COUNCILLORS

1. Principles

Liskeard Town Council (The Council) provides Councillors with access to various facilities for work and communication purposes. To ensure compliance with all relevant legislation and standards in relation to data protection, information security and compliance monitoring, the Council has adopted an Information Technology (IT) Usage & Security policy for Councillors which should be read in conjunction with its Data Protection policy.

2. Breach of the policy

Breach of this policy will be regarded as an offence and may be reported to the Full Council for consideration of further action required.

Anyone who considers that there has been a breach of this policy in relation to personal information about them held by the Council should raise the matter via the Council's formal grievance procedure.

3. Objectives

The Council makes use of IT systems, for data storage, communications and as a source of information. This policy is intended to:

- prevent inappropriate use of computer equipment (such as extended personal use or for accessing and circulating pornographic, racist, sexist or defamatory material);
- protect confidential, personal or commercially sensitive data;
- protect the Council from the risk of financial loss, loss of reputation or libel;
- prevent the introduction of viruses;
- prevent the use of unlicensed software;
- ensure that the Facilities are not used so as to cause harm or damage to any person or organisation
- ensure that Council property is properly looked after; and
- monitor the use of computer facilities to ensure compliance with internal policies and rules and to detect abuse.

4. Usage

This policy sets out the Council's position on your use of the Facilities and it includes:

- your responsibilities and potential liability when using the Facilities
- the monitoring policies adopted by the Council; and
- guidance on how to use the Facilities.

The policy applies to the use of:

- desktop and portable computers, tablets and applications;
- electronic mail and messaging services;
- social media; and
- local, inter-office, national and international, private or public networks and all systems and services accessed through those networks.

5. User Responsibilities

Subject to anything to the contrary in this policy the Facilities must be used for Council business purposes only.

Councillors are granted access only to systems, programs and information necessary to do their job.

It is expressly prohibited from using the Facilities for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Council or its clients other than in the normal and proper course of carrying out your duties for the Council.

To ensure proper use of Council computers, Councillors must adhere to the following practices:

- Anti-virus software must be kept running at all times.
- Do not open attachments or click on links unless you know you can trust the source
- Media storage such as USB drives, CD's or portable hard drives will not be permitted unless they have been authorised for use by the Town Council.
- All devices must be password protected, using password recognised complexity rules, and changed regularly. Do not divulge or write down your password anywhere an unauthorised person could find it, PIN, or other authentication. Change your password immediately if you believe its confidentiality may have been compromised.
- Always log off/screen lock your device whenever you leave it for more than a moment.
- Any breaches or suspected security incidents concerning Council data or computing facilities must be reported immediately to the Town Clerk who is the Data Controller.
- Never knowingly use facilities in a manner which may introduce security or operational risk.
- Never attempt to perform any unauthorised changes to Council IT systems.
- All data held on Council devices and systems may also be subject to Freedom of Information or Subject Access Requests. For this reason, personal use of the Council's computing and network facilities cannot be deemed to be private.
- Do not use or attempt to use another individual's account.
- Never exceed the limits of your authorisation or specific business need by attempting to access systems or information that you do not need in order to carry out your role. A deliberate and intentional attempt to access unauthorised resources breaches the Computer Misuse Act 1990.
- If you believe you have mistakenly been granted access to IT systems, information or resources which are not appropriate or authorised to you, please immediately report this as a possible incident. Do not under any circumstance 'explore' or attempt further access yourself.
- Do not facilitate or attempt to facilitate access for anyone else who is not authorised to access specific information or information systems.
- Never copy, store, or transfer data or software owned by the Council to any unmanaged device without explicit written consent from the Asset Owner.

6. Desktop and portable computers, tablets and applications

All hardware and software issued to Councillors remains the property of the Town Council.

When using such equipment:

- you are responsible for all equipment and software until you return it. It will be insured by the Town Council against loss and damage in accordance with the terms and conditions of the Council insurance, but must be kept secure at all times.
- you are the only person authorised to use the equipment and software issued to you.
- if you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the Council's attention.
- upon the request of the Council at any time, for any reason, you will immediately return any laptop, equipment and all software to the Council.
- if you are using your own laptop or PC to connect with the Council's or to transfer data between the laptop/PC and any of the Council's computers you must ensure that you have obtained prior consent, comply with instructions and ensure that any data downloaded or uploaded is free from viruses; and
- you will be responsible for ensuring that your home equipment is adequately protected from viruses and malware.

7. Software

Software piracy could expose both the Council and the user to allegations of intellectual property infringement. The Council is committed to following the terms of all software licences to which the Council is a contracting party. This means that:

- software must not be installed onto any of the Council's computers unless this has been approved in advance by the Town Council. Before granting approval, the Town Council may seek advice from its IT consultant to ensure that the appropriate licence has been obtained, that the software is virus free and compatible with the computer Facilities; and
- software should not be removed from any computer nor should it be copied or loaded on to any computer without prior consent.

- you will be responsible for ensuring that your home equipment is adequately protected from viruses and malware and that operating system patches are routinely applied.

8. Email (internal or external use)

It is recommended that a separate email address is used exclusively for Town Council business. On request, Liskeard Town Council can provide a liskeard.gov.uk email address for your use.

Internet email is not a secure medium of communication; it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If you are sending confidential information by email this should be sent using password protected attachments where possible.

Email should be treated as any other documentation. If you would normally retain a certain document in hard copy you should retain the email.

Do not forward email messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo with the same information do not forward the email.

Your email inbox should be checked on a regular basis.

As with many other records, email may be subject to discovery in litigation, or a Freedom of Information request. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of the Facilities is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

Councillors with a Town Council issued email account will be required to surrender their email account and all of its contents to the Town Clerk at the end of their term of office or if they decide to leave the Council.

Further guidance can be found in the Liskeard Town Council Communications Policy.

9. Social Media

Councillors using their own social media accounts must ensure that any comment made is clearly identified as their own and not representative of the Council.

Full guidance can be found in the Liskeard Town Council Social Media Policy

10. Internet

Posting information on the internet, whether on a newsgroup, via a chat room or via email is no different from publishing information in the newspaper. If a posting is alleged to be defamatory, libellous, or harassing, the person making the posting and the Council could face legal claims for monetary damages.

Using Council internet facilities for the purpose of trading or carrying out any business activity other than Council business is strictly prohibited.

For the avoidance of doubt the matters set out above include use of wireless facilities.

11. Monitoring policy

The policy of the Council is that we may monitor your use of the Facilities.

The Council recognises the importance of an individual's privacy but needs to balance this against the requirement to protect others and preserve the integrity and functionality of the Facilities.

The Council may from time to time monitor the Facilities. Principal reasons for this are to:

- detect any harassment or inappropriate behaviour by employees and Councillors, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex discrimination policies;
- ensure compliance of this policy;
- detect and enforce the integrity of the Facilities and any sensitive or confidential information belonging to or under the control of the Council;
- ensure compliance by users of the Facilities with all applicable laws (including data protection), regulations and guidelines published and in force from time to time; and
- monitor and protect the wellbeing of employees and Councillors.

The Council may adopt at any time a number of methods to monitor use of the Facilities.

These may include:

- recording and logging the activities by individual users of the Facilities. This may include opening emails and their attachments, monitoring Internet usage including time spent on the internet and websites visited;
- physical inspections of individual users computers, software and telephone messaging services;
- periodic monitoring of the Facilities through third party software including real time inspections;
- physical inspection of an individual's post;
- recording and logging of internal, inter-office and external telephone calls made or received by employees and Councillors using its telephone network (including where possible mobile telephones). Such recording may include details of length, date and content;
- and archiving of any information obtained from the above including emails, telephone call logs and Internet downloads.

The Council will not (unless required by law):

- allow third parties to monitor the Facilities (with the exception of our appointed IT consultant); or
- disclose information obtained by such monitoring of the Facilities to third parties unless the law permits.

The Council may be prohibited by law from notifying employees using the Facilities of a disclosure to third parties.

Observation of this policy is mandatory and forms part of the terms and conditions of of access to Liskeard Town Council's equipment, systems and offices. **Misuse of the Facilities will be treated as gross misconduct and actioned accordingly.**