MINEHEAD TOWN COUNCIL

ICT POLICY

REVIEWED

Minehead Town Council

ICT Policy

1. Policy Statement.

This policy describes the acceptable use of all ICT equipment and facilities within Minehead Town Council.

Inappropriate use of our ICT facilities heightens the risks of data loss, system outages due to virus and other malware attacks, financial loss and legal issues.

Failure to comply with this policy may result in ICT facilities being withdrawn and disciplinary action being taken.

The policy applies to everyone, including contractors and visitors, who uses Council owned or leased information technology equipment and telecommunications networks.

2 Monitoring and Privacy.

Users of our ICT facilities have a reasonable expectation of privacy in terms of how they use those facilities. However, to assure the security of our data, and to enable investigations to take place in the event of a security incident, monitoring of ICT usage does take place.

The information gathered for monitoring purposes includes information that falls into the personal data category and as such the requirements of the Data Protection Act 2018 apply to our handling and processing of this data. The legal basis for processing of personal data for the purpose of monitoring ICT usage is based on legitimate interest, and our processing of this data will be proportionate and carried out in the least intrusive manner reasonably possible.

This policy allows for 'reasonable' personal use of some ICT facilities, but users should be aware that monitoring systems do not differentiate between business and personal use – all use is monitored in the same way.

3 Prohibited activities whenever using Council ICT and services.

The following activities are prohibited – you should not knowingly:

• offend, insult, harass, threaten, or deceive other people.

• request, create, access, store, or send offensive, pornographic, indecent, or illegal material.

• breach copyright or licence agreements

• connect unauthorised devices to Council ICT or networks.

• connect Council mobile devices to unauthorised computers.

• download, use, or distribute unauthorised software or applications.

• remove, disable, or nullify operational components, safety, or security measures in Council ICT.

• try to misuse, gain unauthorised access to, or prevent legitimate access to, any ICT equipment, network, system, service, or account.

• try to gain unauthorised access to information, or release information without proper authority.

• bring the Council into disrepute or obstruct its business.

• be negligent in protecting the ICT and services, or the information you can access from it.

• break the law or encourage others to do so.

Please be aware that the above activities could be treated as gross misconduct in any disciplinary proceedings that may follow.

4 Personal use of Council ICT.

The Council allows you limited personal use of its ICT (although this can be stopped at any time at the Council's discretion). When making personal use of Council ICT, you must not:

• use Council equipment for inappropriate personal use (for example, streaming videos or gaming) take part in personal commercial activity including, but not limited to, peer-to-peer marketing.

• make personal purchases from websites (including auction sites)

• undertake any form of share dealing.

• take part in any gambling or lottery.

• store any personal data or information on Council devices.

• waste Council time, money, or resources.

The Council does not accept any liability for any loss, damage or inconvenience you may suffer as a result of personal use of its ICT and services.

5 Information Security.

Protecting the security of information stored on our computer systems is of critical importance. The following must be observed to support this:

• Passwords should always be kept secure, and not shared with others.

• Your device should be locked when unattended

• You must not use systems unless logged in using your own login credentials. The only exception to this is to enable ICT support staff to perform legitimate support activities.

• Security incidents must be promptly reported.

• Great care must be taken when posting to social media platforms (e.g. Slack, WhatsApp, Facebook, Twitter etc). These sites are not compliant with our obligations under data protection and so you must not post information that should not be in the public domain or transact business via these sites (unless as part of your role through official Minehead Town Council accounts).

Please be aware that if a data breach occurs that requires the involvement of the Information Commissioner, the individual responsible for the data breach may be subject to enforcement actions, including their name being released in the public domain. As well, if you use social media platforms for sharing work information, these are disclosable under the Freedom of Information Act 2000 as well as the Data Protection Act 2018 (for subject access requests).

6 Mobile Phones/Tablets/Laptops.

Mobile phones,tablets or laptops are issued based on business need and should be used in accordance with this policy document. Devices are issued for work purposes and should not be shared with anyone else including colleagues, family, or friends.

6.1 Software Updates.

Periodically, software updates are issued by Apple and Android to fix bugs/security issues and add new features. Therefore, you should update your device with new software as soon as reasonably possible.

6.2 Voice / Data Tariff.

There is no default Voice/Data contract supplied with devices. It is the responsibility of individual staff members to make themselves aware of the voice/data tariff of their assigned device.

6.3 Wi-Fi.

Secure Wi-Fi is provided at the Council Offices, and this should be used in preference to 3G/4G whenever in range.

If working from home, your home Wi-Fi should be used whenever possible. If you do not have home Wi-Fi which is sufficient to allow working from home without using mobile data, you must talk to the Clerk about this to agree a solution.

Use of unsecured, open Wi-Fi hotspots presents a heightened risk as hackers are more easily able to intercept data transmitted via these hotspots. Therefore, if you are using one of these hotspots you must ensure that information sent over the network is encrypted – either via the VPN system on a laptop, or via an appropriate app on a smartphone/tablet.

6**.4 Personal Use.**

The device should not be used to replace personal devices, but reasonable personal use is acceptable, subject to the following:

• The device is provided to support the business needs of the organisation and user. Personal use must not impair this.

Examples of use that may use large amounts of data include (but are not limited to):

Streaming or downloading television / films to the device

Online gaming

Use as personal hotspot for other devices.

6.5 Limitations on Use.

• The device should not be used outside of the UK.

• Personal / Sensitive Council data should not be stored on the device, unless pre-agreed with the Clerk.

• Picture Messaging / MMS – as all MMS messages are separately chargeable then this service should not be used

6.6 Lost or Stolen Device.

If a device is lost or stolen, then it needs to be wiped as soon as possible to minimise the risk of data loss. The Council should be contacted as soon as possible to report the loss.

6.7 Purchasing / issuing new devices.

Devices are issued to users based on business need, via an agreed process, and so new devices must only be purchased via the permission of the Clerk.

Devices should be returned to the Council once no longer needed (e.g. if the current owner leaves the Council). They must not be given to other users directly as there is a need to ensure the device is wiped and correctly configured for a new user. The Council will keep the policy about business need for new devices under review.

6.8 Health and Safety.

The use of mobile telephones as a means of communication is encouraged but precautions must be taken to avoid excessive use. All mobile telephones purchased will meet international standards. The following advice should be observed when using a mobile phone:

- Do not use mobile phones in the vicinity of sensitive electronic equipment, where there could be an explosive atmosphere or where it might cause a nuisance to others.

• Keep the batteries charged and an emergency number programmed into the memory.

Formatted: Justified

• Avoid any risks associated with prolonged use by putting calls on speaker, using earphones or hands-free kits.

All staff and Councillors are reminded that it is an offence for a driver to use a hand-held mobile phone in the vehicle at any time when the engine is running. This includes when stationary at traffic lights or when parked on or adjacent to roads when the engine is running.

No Minehead Town Council employee or Councillor should use a mobile phone whilst in the driving seat of a vehicle and the engine is running. There are three exceptions to this rule:

• if your life is in danger and you need to contact emergency services on 999 and to stop would exacerbate the situation

• if the mobile phone system can be activated entirely 'hands free'. Any such calls must be kept to an absolute minimum and the driver must stop the vehicle in an appropriate and safe place before calling back under any circumstances.

• Use of the mobile phone as a navigation tool. This must be set up before the journey starts and the phone must not be used while driving.

Remember, no telephone call is so urgent that it can be allowed to jeopardise personal or road safety.

The Road Safety Act can penalise drivers who cause death by careless driving whilst carrying out an avoidable activity (texting/calling/drinking/eating) with significant custodial sentences as well as fines.

7 Home / Flexible Working.

Our operating model encourages staff and Councillors to work from their place of work.

There is an element of flexibility to work from home, or other non-office locations. When working in this manner, the following should be observed:

• Keep usage to a minimum in public areas.

• Only use information for work related purposes.

• Ensure the security of information.

• Keep equipment and files locked out of sight during transit.

• Only store data on council-provided or ICT-approved equipment

• Do not send council data to personal email addresses or private internet storage sites (e.g. Dropbox, Google Drive) unless specific authorisation for this has been obtained.

Ensure that family members or visitors to your home are not able to access equipment or data.

8 Personal Devices.

Personal devices (including USB devices) are only permitted to access council data or systems on pre-agreement from the Clerk.

Personal mobile phones used by Amenities Operatives can only be used for Minehead Town Council business if pre-agreed by the Clerk.

The Council will keep this policy under review as our corporate systems change, which may enable safe use of personal devices to access some systems.

I have read and agree to comply with the policy.

Name: _____ Date: _____

Please return to the Minehead Town Council Office, 3 Summerland Road, Minehead, TA24 5BP