PORTISHEAD TOWN COUNCIL

Acceptable Use of IT Policy

Purpose

This Acceptable Usage Policy covers the security and use of all of Portishead Town Council's (the Council) information and IT and telephone equipment (facilities), that include email, internet, voice and mobile facilities. This policy applies to all Council employees, contractors and agents (hereafter referred to as 'individuals').

The purpose of the policy is to ensure compliance with all applicable laws in relation to GDPR, Data Protection, information security and compliance monitoring. In addition, to protecting the Council from risk of financial loss, loss of reputation or libel.

The policy sets out the Councils position on:

- responsibilities and potential liability when using the facilities
- the monitoring process adopted by the Council
- guidance on how to use the facilities

This policy applies to the use of:

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

Breach of the policy

Breach of this policy will be regarded as a disciplinary offence and will be dealt with under the Council's Disciplinary Procedure. Anyone who considers that there has been a breach of this policy should raise the matter with the Town Clerk or via the Council's Grievance Procedure.

Computer facilities: Use of computer systems

To maintain the confidentiality of information held on or transferred via the Council's facilities, security measures are in place and must be followed at all times. A log-on ID and password is required for access to the Council's network. This will be changed regularly and must be kept secure.

You are expressly prohibited from using the facilities for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Council

other than in the normal and proper course of carrying out your duties for the Council.

The Council provides the Facilities solely for the purposes required for the performance of job responsibilities in the conduct of Council business. Occasional and reasonable personal use of the Facilities is permitted, including personal calls that are important or urgent, provided this does not interfere with work performance, security, confidentiality or any other aspect of this policy.

The Facilities must not be used to access personal social media or for gambling, personal shopping or trading purposes.

In order to ensure proper use of Council computers, you must adhere to the following practices:

- anti-virus software must be kept running at all times
- media storage such as USB drives, CD's or portable hard drives will not be permitted unless they have been provided by the Council
- obvious passwords such as birthdays and spouse names, etc., must be avoided (the most secure passwords are random combinations of letters and numbers)
- all files must be stored on the network drive which is backed up regularly to avoid loss of information
- individuals must not leave their user accounts logged in at an unattended computer and should always log off overnight
- passwords are not to be written down, left unprotected and are not be used or shared by others
- individuals are not to perform any unauthorised changes to the Council's IT systems or information
- individuals must not store personal files such as music, video, photographs or games on Council IT equipment
- individuals must not attempt to access data that they are not authorised to use or access or exceed the limits of their authorisation or specific business need to interrogate the system or data
- data or software is not to be given or transferred to any person or organisation outside of Portishead Town Council without permission
- only agreed email signatures may be used
- confidential material should not be disclosed
- only attachments from a trusted source may be downloaded
- emails should not be re-circulated without the senders consent

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car
- Laptops must be carried as hand luggage when travelling
- Information should be protected against loss or compromise when working remotely (for example at home or in public places)
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data.

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, in particular, that:

Software must not be installed onto any Council computer unless this has been approved in advance by the Councils IT Contractors. They will be responsible for establishing 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.

Laptop computers, PC's , tablets and smart phones

Laptop computers, PC's, tablets and smart phones belonging to the Council along with related equipment and software are subject to all of the Council's policies and guidelines governing non-portable computers and software. When using such equipment:

- you are responsible for all equipment and software until you return it. It must be kept secure at all times

- you are the only person authorised to use the equipment and software issued to you

- you must work within the shared network environment when carrying out Council business to ensure that all data is backed up and accessible by the Clerk

- 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 equipment and all software to the Council; and

- if you are using your own laptop or PC to connect with the Council's network or to transfer data between the laptop or 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.

Email (internal or external use)

All staff will be issued a Council email account which should be used when transacting on behalf of the Council.

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.

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 paper correspondence with the same information do not forward the email.

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

Viewing, displaying, storing 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.

Staff will be required to surrender their email account and all of its contents to the Clerk if they decide to leave the Council.

When using email or sending any form of written correspondence:

- be careful what you write; never forget that email and written correspondence are not the same as conversation: they are a written record and can be duplicated at will

- use normal capitalisation and punctuation; typing a message all in capital letters is the equivalent of shouting at the reader

- check your grammar and spelling

- emails and other forms of correspondence should maintain the high standards expected by the Council.

Monitoring

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

- detect any harassment or inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex discrimination policies

- ensure compliance to 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

Portishead Town Council has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000 and the 2018 GDPR.

This policy must be read in conjunction with:

- Computer Misuse Act 1990
- Data Protection Act 1998
- GDPR 2018

The Council will not (unless required by law):

- allow third parties to monitor the facilities (with the exception of an appointed IT supplier); 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.

Approved at the meeting held on xxxxxx