



IT Policy

Contents

1.0 Introduction

2.0 Roles and Responsibilities

3.0 General IT Policy

3.1 Account Access (Request and Leavers)

3.2 Computer Security

Data Security

Passwords

Screen Locking

Lost or Stolen Equipment

Memory Stick and Removable Media

Viruses

Emails

Out of Office

Internet

Monitoring

3.3 Bring Your Own Device (BYOD)

4.0 References to other policies



IT Policy

1.0 Introduction

Pontypool Community Council (PCC) has a duty to ensure the proper security and privacy of its computer systems and data.

The document sets out the procedures and responsibilities of everyone using IT at PCC, this includes Staff and Councillors.

It should be noted that PCC use an external IT company for all IT support – Custom Computer Services Wales (CCSW). CCSW can be contacted via phone 0333 014 4544, alternatively issues can be logged via the online portal:-
<https://ccsw.servicedesk.atera.com/tickets>

All new equipment and disposal of old equipment will be done directly through CCSW as these are the approved IT provider for PCC. Upon disposal of equipment PCC will receive a destruction certificate from CCSW, at this point the asset should be removed from the PCC asset register.

The scope of the policy also covers requirements for Cyber Essentials certification.

2.0 Roles and Responsibilities

The Clerk is responsible for the implementation and monitoring of this policy but may delegate that responsibility as needed.

Line managers have a responsibility to ensure staff they supervise comply with this policy.

The Finance Manager or delegate is responsible for ensuring that the PCC asset register is kept updated when new laptops are bought and old ones are removed for disposal.

All Staff should receive appropriate training on IT security as part of their induction and regular training as deemed appropriate. As a minimum staff should undertake, GDPR and Display Screen equipment training.

3.0 General IT Policy

3.1 Account Access (Request and Leavers)

Access to the PCC system is authorised by the Clerk or delegate, for new staff members upon their induction by completing a new starter form in the CCSW online portal and for new councillors when they have signed their declaration paperwork again via CCSW.

All new staff and Councillors will be assigned a Council email address, this should be used for all Council work and should not be used to send inappropriate material.



IT Policy

The Clerk or delegate will complete a leaver form in the CCSW online portal for all Councillors and Staff that need to have access to the system suspended. Ideally this should be on the day that the person leaves. The Clerk or delegate must ensure that the users work related information, e-mails and data is transferred, if required, to the respective working directory for future access on the system, or is deleted. This will ensure that the appropriate security is maintained on leavers information and data.

Return of IT equipment

When an employee leaves PCC, the Clerk or delegate must ensure all IT equipment is returned by either:

- Arranging items to be collected. or ;
- On the last working day, Managers must collect all the leavers IT equipment and ensure it is returned and stored appropriately.
- Failure to comply with the requirements of this policy in relation to the return of IT equipment is regarded as a serious breach of this policy.

3.2 Computer Security

Data Storing

All Staff must abide by the rules of the Data Protection Act and GDPR policies.

All PCC related work should be stored on the Pontypool Community Council shared cloud drive as this is regularly backed up and therefore is resilient to failure.

Individuals can choose to save documents on their own One Drive but these documents cannot then be shared with other PCC users.

Unauthorised access to any of the Councils computer systems will amount to gross misconduct for employees, a report to the Ombudsman for Councillors, and prosecution for members of the public.

Unauthorised copying and/or removal of computer equipment/software will result in disciplinary action; such actions could lead to dismissal.

Passwords

All Staff and Councillors need to ensure passwords are protected and not to disclose them to other individuals.

A computer password is an important piece of confidential information and it should be treated that way. The password should not be shared with others and it should not be written down anywhere where an unauthorised person can find it.

Passwords must conform to the following criteria:-

- Minimum 8 characters



IT Policy

- Comprise of at least one upper case letter, one lower case letter and one number. Where possible, two factor authentication should be used.

Screen Locking

Computers should not be left unattended, when leaving your computer ensure the screen had been locked, and that an auto lock after 10mins has been applied.

Lost or stolen equipment

CCSW should be contacted immediately if a laptop has been lost or stolen so that the device can be suspended so that it can no longer be used. Replacement equipment should be sought with approval from the Clerk or delegate.

Memory Sticks and Removable Media

Memory sticks are not to be used at PCC for storing of documents that are being worked on by individuals – Staff should ensure their One Drive is used for such items, so that documents can be retrieved when necessary. Memory sticks should also not be used for transferring data from Councillors or members of the public to staff laptops – this is a breach of this policy.

Viruses

In order to prevent the introduction of viruses users should refrain from intentionally sending and downloading files or attachments which may contain viruses. If a virus is suspected CCSW should be informed immediately.

All files received from outside PCC will be checked for viruses using installed software.

New software requested by Staff or Councillors must be authorised by the Clerk or delegate (in liaison with CCSW).

Emails

The use of the e-mail system is encouraged as its appropriate use facilitates efficiency. Used correctly it is a facility that is of assistance to employees. Inappropriate use however causes many problems including distractions, time wasting and legal claims. The below sets out the Council's position on the correct use of the e-mail system.

Unauthorised or inappropriate use of the e-mail system may result in disciplinary action which could include summary dismissal.

The e-mail system is available for communication and matters directly concerned with the legitimate business of the Council. Employees using the e-mail system should give particular attention to the following points:



IT Policy

- a) all comply with Council communication standards;
- b) e-mail messages and copies should only be sent to those for whom they are particularly relevant;
- c) e-mail should not be used as a substitute for face-to-face communication or telephone contact. Abusive e-mails must not be sent. Hasty messages sent without proper consideration can cause upset, concern or misunderstanding;
- d) if the e-mail is confidential the user must ensure that the necessary steps are taken to protect confidentiality. The Council will be liable for infringing copyright or any defamatory information that is circulated either within the Council or to external users of the system; and
- e) offers or contracts transmitted by e-mail are as legally binding on the Council as those sent on paper.

The Council will not tolerate the use of the e-mail system for unofficial or inappropriate purposes, including:

- a) any messages that could constitute bullying, harassment or other detriment;
- b) personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters);
- c) on-line gambling;
- d) accessing or transmitting pornography;
- e) transmitting copyright information and/or any software available to the user; or
- f) posting confidential information about other employees, the Council or its clients or suppliers.

Staff and Councillors are issued with a standard sized mailbox, once the mailbox limit has been reached users of that mailbox will not be able to send or receive any further mail and therefore regular housekeeping of emails must be planned well in advance of reaching the space limit. When choosing email that are to be kept, the document retention policy should be referred to. All other email that is not necessary for the business should be deleted once it is no longer required.

Out of Office

An "Out of Office" notice must be used whenever a member of Staff is away and should indicate a date of return and contact details for those who can deal with issues whilst the individual is away. If a member of Staff or Councillor is away and has not actioned an out of office message, CCSW can be contacted to set one up.

Internet



IT Policy

Where appropriate, duly authorised staff are encouraged to make use of the Internet as part of their official and professional activities. Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in the Council name. Where personal views are expressed a disclaimer stating that this is the case should be clearly added to all correspondence. The intellectual property right and copyright must not be compromised when publishing on the Internet. The availability and variety of information on the Internet has meant that it can be used to obtain material reasonably considered to be offensive. The use of the Internet to access and/or distribute any kind of offensive material, or material that is not work-related, leaves an individual liable to disciplinary action which could lead to dismissal.

Procedures – Acceptable/Unacceptable Use

Unauthorised or inappropriate use of the internet system may result in disciplinary action which could result in summary dismissal.

The internet system is available for legitimate business use and matters concerned directly with the job being done. Employees using the internet system should give particular attention to the following points:

- a) comply with all of our internet standards;
- b) access during working hours should be for business use only; and
- c) private use of the internet should be used outside of your normal working hours.

The Council will not tolerate the use of the Internet system for unofficial or inappropriate purposes, including:

- a) accessing websites which put our internet at risk of (including but not limited to) viruses, compromising our copyright or intellectual property rights;
- b) non-compliance of our social networking policy;
- c) connecting, posting or downloading any information unrelated to their employment and in particular pornographic or other offensive material; or
- d) engaging in computer hacking and other related activities, or attempting to disable or compromise security of information contained on the Council's computers.

You are reminded that such activities (c and d) may constitute a criminal offence.

Monitoring

PCC reserve the right to monitor all e-mail/internet activity by you for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements. This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks, which are



IT Policy

subject to the same rules as your work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings. Monitoring your usage will mean processing your personal data. You may read more about the data we hold on you, why we hold it and the lawful basis that applies in the employee privacy notice.

3.3 Bring Your Own Device (BYOD) Policy

This section defines procedures that are in place to ensure BYOD devices are compliant with the PCC security policy. Staff and Councillors are permitted to use their own Smartphones to access emails/, calendars, Teams, documents etc. However, in order to prevent unauthorised access, the device must be password protected. The device should lock itself with a password or pin after 10minutes being idle.

4.0 References for other Policies

- Social Media Policy
- Data Protection Policy
- Retention of Documents Guidance
- Staff Handbook