Version No.	3
Adopted Date:	January 2024
Last Reviewed Date:	September 2026
Next Review Date:	September 2028

ARTIFICIAL INTELLIGENCE AND IT POLICY

1 Introduction and Purpose

1.1 This policy sets out the Council's approach to the use and management of:

- Artificial Intelligence
- IT

2 Artificial Intelligence (AI)

2.1 Use of AI

2.1.1 We recognise that the use of AI is on the increase and has been harnessed by some organisations to save time and resources and enhance the user experience. Artificial intelligence refers to computer systems that can think or act in a more human way, taking information from their surroundings to perform tasks that usually require human intelligence.

2.1.2 Freely available AI platforms are rapidly multiplying and this policy applies to all forms of AI, including AI Assistants & Chatbots (e.g. ChatGPT, Claude, Gemini, DeepSeek, Grok, Zapier Agents), Video Generation & Editing (e.g. Synthesia, Runway, Filmora, OpusClip, Descript), Image Generation (e.g. Midjourney, DALL·E 3, Canva Magic Studio, Looka, Pixlr), Writing & Content Creation (e.g. Rytr, Sudowrite, Jasper, Anyword, Writer, Grammarly, Wordtune, ProWritingAid, SEO AI, Copy.ai) Coding & Development (e.g. GitHub Copilot, Cursor, Codeium, Amazon CodeWhisperer, CodyAI, Cursor, Qodo) Notetaking & Meeting Assistants (e.g.Fathom, Nyota, Fireflies, Avoma, tl;dv), Search Engines (e.g. Perplexity, ChatGPT search, Google AI Overviews, Arc Search)

2.1.3 ChatGPT is an example of an AI chatbot that can provide answers to questions a user asks it. It can create content formatted in accordance with specific instructions. Although there are multiple benefits to using ChatGPT, it can be problematic when used in the workplace. Therefore, we have set out below our rules on the use of ChatGPT and other AI platforms, both as part of your role and in your own time, in order to protect our business interests.

2.2 Risks associated with the use of ChatGPT and AI

2.2.1 By the admission of its own creators (OpenAI), ChatGPT has its limits. For example, it can:

- give an incorrect answer to the question asked;
- give inconsistent answers when asked the same question more than once;
- provide outdated information;
- provide information that is biased or discriminatory;
- create a security or data protection risk when confidential information is inputted.

2.2.2 In addition, AI can engineer a false view of someone's capabilities when the information it provides is used inappropriately.

2.3 Using AI

2.3.1 You are permitted to use AI to carry out your tasks. However, you must be aware of the risks as set out above. You remain entirely responsible for the quality and accuracy of your work.

2.3.2 Failure to maintain the required quality and accuracy of your work may result in the initiation of disciplinary or capability procedures.

2.3.3 Whether during your work activity or in your own time, you must not input any information into AI platform that:

- identifies our organisation either directly or indirectly;
- is reasonably considered to be confidential or sensitive organisation information including any content that you have created as part of your work.

2.3.4 This is because AI learns from the information that is inputted and can provide information to subsequent users based on the information it receives.

2.4 Confidential or Sensitive Information

2.4.1 Where referred to above, "confidential or sensitive information relating to our organisation" includes, but is not limited to:

- Information about employees;
- Information about customers/clients/suppliers/service users;

- Financial information;
- Internal policies and procedures;
- Software code;
- Any other information which may identify the Council.

3 IT

3.1 Security and Privacy

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

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

3.1.3 It should be noted that PCC uses 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 or by emailing ticket@CCSW.co.uk.

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

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

3.2 Roles and Responsibilities

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

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

3.2.3 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.

3.2.4 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.

3.3 Account Access (Request and Leavers)

3.3.1 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.

3.3.2 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.

3.3.3 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 user's 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.

3.4 Return of IT equipment

3.4.1 When an employee leaves the Council, 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.

3.5 Computer Security

3.5.1 **Data Storing:** All Staff must abide by the rules of the Data Protection Act (2018) 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.

3.5.2 **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;
- comprise of at least one upper case letter, one lower case letter and one number.

Where possible, two factor authentication should be used.

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

3.5.4 **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.

3.5.5 **Memory Sticks and Removable Media:** Memory sticks are not to be used at the Council 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.

3.5.6 **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).

3.5.7 **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:

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 emails 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.

3.5.8 **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.

3.5.9 **Internet:** 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's 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.

3.6 Procedures – Acceptable/Unacceptable Use

3.6.1 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.

3.6.2 **Monitoring:** the Council 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 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.

3.7 Bring Your Own Device (BYOD) Policy

3.7.1 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 10 minutes being idle.

3.8 References for other Policies

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