Internet Acceptable Use Policy

Internet Acceptable Use Policy Objective

This Internet Policy shall apply to all Pontypridd Ministry Area (PMA) employees. The objective of the Internet Acceptable Use Policy (AUP) is to ensure the safe, effective and appropriate use of the Internet facilities. While PMA is committed to the use of the Internet for business/ministry purposes, it must ensure that suitable controls are in place to prevent security breaches or other negative consequences. The primary use of the Internet is for business/ministry purposes. This policy has been developed to manage the way in which the authority complies within the ISO 27001 standard.

Scope
Internet access refers to the use of any resources from the World Wide Web, whether browsed or downloaded.
Internet access provided by PMA refers to business provided access, Wi-Fi, Guest/Visitor Wi-Fi, and communities network access.

Policy Statements
PMS's Internet facilities shall be used in accordance with:
• PMS's specified and published principles and policies;
• All appropriate legislation.

Internet usage on official PMA sites may be monitored to ensure compliance with this Internet AUP. Any updates will be passed to full Council for approval.

Implementation responsibilities
The Information Security Officer shall develop, maintain, and publish processes to achieve compliance with this Internet AUP.
All employees shall be responsible for implementing the Internet AUP within their areas of responsibility.
All employees shall sign the Information Security Policy to indicate their agreement to comply with the Internet AUP.

The PMA Leader or Operations Manager, are authorised to update and amend the Information Security Policy which must be ratified by the PMA Council.

Internet Usage Principles

1. Due to the structure of the PMA, it is assumed that all employees will need to access the internet in for work purposes.

2. Official PMA sites will have PC's connected to the Wi-Fi for use in connection with PMA duties.

3. Messages or images shall not be posted on any Internet, Intranet, message board or other similar Web based service that would bring PMA into disrepute, or which a reasonable person would consider to be offensive or abusive.

4. Internet users shall not place on the Internet or Intranet any opinion or statement that might be construed as representing PMA.

5. Internet access shall not be used for financial gain, or to host any unauthorised website on any PMA equipment.

6. PMA shall report any illegal activity to the Police. Employees shall also be liable to PMA's own disciplinary process, and clerics will be referred to the Disciplinary Tribunal of the Church in Wales.

7. Internet users shall not participate in on-line games or have active any web channels that broadcast frequent updates to their computer. They shall not access any social media sites other than those approved for work purposes.

8. Internet users should not visit Web sites that display material of pornographic nature, or which contain material that may be considered offensive. Employees shall notify the Ministry Area Leader er immediately should accidental access to such material occur. No disciplinary action shall be taken against employees who accidentally access sites containing dubious or unethical material providing they advise the Ministry Are Leader in a timely manner. However, in order to avoid disciplinary action, it is the Internet users' responsibility to ensure that such unauthorised access does not happen on a frequent basis.

The following is not an exhaustive list but an indication of the types of conduct that may result in disciplinary action and possibly dismissal and is deemed unacceptable use or behaviour by employees:

- Visiting Internet sites that are illegal, obscene or libellous;
- Visiting sites that are offensive, abusive, sexist, racist, hateful, defamatory or annoying;
- Gaining access to unauthorised areas ('hacking');
- Infringing another person's/organisation's copyright and/or other statutory, regulatory and/or current law prescriptions;
- Using the computer and/or Internet to perpetrate and form of fraud, or software, film or music piracy;
- Transmission of unsolicited commercial or advertising material;
- Obtaining unauthorised access to PMS's ICT facilities;
- Violating other people's privacy;
- Using chat lines or similar services;
- Playing games;
- Illegal activities including breaching Data Protection Laws, Computer Misuse and Design Copyright and Patents Acts;
- Wasting network and staff resources;
- Disrupting other user's work in any way, including by viruses or data corruption;
- Expressing personal views, which could be misinterpreted as those of PMA;

- Committing PMA to purchase or acquiring goods or services without proper authorisation;
- Downloading copyrighted or confidential information;
- Using the Internet to an excessive degree. If the line manager considers that the Internet is being used more than is necessary for the business function then the facility may be withdrawn;
- Posting defamatory, offensive, abusive, sexist, racist or annoying comments on the PMA's social media or internet site;
- Creating or supporting any Internet messages or postings that are intended to harass, annoy or alarm any person or organisation;
- Publishing defamatory and/or knowingly false material about the PMA, clerics, members of staff, volunteers, parishioners or service users on social networking sites, blogs, online journals or any online publishing format;
- Revealing confidential information about the PMA, its staff, clerics, volunteers', parishioners, or service users, in a personal online posting, private messaging, upload or transmission – including financial information, business plans, policies, staff and/or internal discussions;
- Introducing any form of malicious software into any of the Council's networks;
- Using personal web-based email to conduct PMA business. The PMA will provide you with a web-based email address;
- No member of staff is permitted to use the PMA Internet access, at any time, for private business activities.

9. Misuse: this includes, but is not limited to, excessive time, large downloads, games, chat rooms, discussion groups, movies or film clips, advertising personal goods or services, online trading, sending unsolicited email (the practice known as 'spamming') and the introduction of unauthorised software to the system.

10. Inappropriate use: this includes, but is not limited to, pornographic or adult-orientated websites or emails, racist, sexist or gambling websites or emails, sites promoting violence, and illegal software.

11. Where material is obtained from the Internet, ensure that any copyright restrictions are obeyed and that virus protection procedures are followed. Where material PMA owns is published, ensure that it carries out copyright indications.

12. Any Internet user using PMA facilities to access offensive material will face disciplinary action if they access such data/material deliberately. If illegal material is accessed deliberately, then PMA will inform the Police and a criminal prosecution may follow.

13. Internet users who attempt to access a website that is blocked by the filtering system but feel that they have a business requirement to access the site, must contact the MAL.

14. Internet users shall not download any files or software from the Internet or capture any images that are displayed as there may be any number of issues concerning copyright, malicious software and overall functioning of the system.

15. Internet users shall not enter their PMA email address on a Website unnecessarily as this might expose PMA to security risks such as malicious software attacks or unwanted junk messages.

16. Internet users logged in at a computer shall be considered to be the person browsing the Internet. Under no circumstances shall Internet users browse the Internet from an account belonging to someone else.

17. All business-related information produced, collected and/or processed in the course of PMA work remains the property of the PMA.

18. PMA has a social network presence which includes Facebook, Instagram, TicTok and YouTube. This presence is not limited to accounts created by the Operations Manager and Ministry Area Executive team – some individuals in service areas have created an online presence on the most popular platforms however this policy prohibits such activity. All social network accounts must be approved by the MAL.

19. Zoom was a popular way of staying in touch during the Pandemic. Zoom Accounts were created by individual locations across the MA. For Safeguarding purposes, all such accounts must cease to exist and all Zoom Activity needs to be hosted by the official PMA account only.

20. Once anything has been published on the Internet, it is extremely difficult to have it removed or to control how it is shared. PMA data must be protected, therefore confidential and restricted information is not uploaded into or shared through social networks as these are inherently insecure.

21. During business hours, staff must only use social network platforms for business purposes.

22. Comments posted on the PMA social network accounts by members of the public that directly relate to a service or project, will be passed on to the appropriate leader (clerical or lay). It is the responsibility of the service to provide the relevant information to clarify the customer query/comment.

23. Employees, clerics and the lay leaders must remember that they are representatives of PMA and using personal social network accounts to make libellous, slanderous or defamatory comments regarding PMA or its employees or clerics will not be tolerated and may lead to disciplinary action.