

Cork County Public Participation Network

Email and Internet Use Policy (P11)

1. What this Policy is for

The PPN is committed to ensuring Internet, email and social media usage that protects all individuals' right to privacy, ensures dignity at work for all employees, and protects the organisation and its interests, including Cork County Council as its host.

Specifically, this purpose is intended to:

- 1.1. ensure that the PPN has clear policies outlining its Internet, email and social media use
- 1.2. set out practical guidelines for transferring person-identifiable information (information which could be used to establish the identity of an individual)
- 1.3. outline procedures in relation to social networking

2. What and who this policy applies to

This policy applies to all email, internet and social media use through the PPN's internet system or on any work hardware used in or out of work premises. It applies to all staff, visitors and volunteers within the PPN.

3. General security

- 3.1. Staff members must not leave their work computer without securing it by password or signing off.
- 3.2. If a staff member thinks that someone knows their password, they must ask for it to be changed as soon as possible. Maintaining the privacy of passwords is individual staff members' responsibility and consequently they are responsible for any abuse taking place using their name and password.

4. Using email, the Internet and social media channels

- 4.1. The PPN email system is to be used solely for the purposes of the PPN and not for personal purposes.
- 4.2. Staff are permitted to use the Internet for personal purposes at work during their breaks and must abide by the Council's Internet policies at all times.
- 4.3. If staff use the PPN or the Council's communications facilities for private purposes, they must accept that those private communications may be subject to surveillance, for example, to ensure adequate virus checking.
- 4.4 All communications must comply with current GDPR regulations (see separate policy)

5. Sending PPN Emails

- 5.1. Email is effectively a communication on official headed paper and can be traced back to place, date and time of sending. Staff, or any person with access to PPN email(s), need to ensure they are satisfied with email content and that it has been approved at the appropriate level. Important email correspondence should use the 'confirm receipt' function.
- 5.2. Staff, or any person with access to PPN email(s), are not to instigate or forward unofficial mail to any users which may be offensive or disruptive to others, or may be construed as harassment.
- 5.3. Staff are not to use another's email account or allow another employee to send from their email account. If sharing computers in an office, then staff are to log off when leaving the computer.

6. Opening Emails

- 6.1. Staff, or any person with access to PPN email(s) must not;
 - open any files that look suspicious or are from an unknown sender
 - reply to any "spam" mail

6.2. If staff, visitors or volunteers receive material which they find offensive or abusive or time-wasting, they should respond to it as to an offensive letter: complain directly to the sender and bring it to the attention of the sender's employing organisation in an appropriate way.

7. Inappropriate Email and Internet Use

7.1. Emails and social media posts may not contain statements or content that is libellous, offensive, harassing, illegal, derogatory, or discriminatory. Inappropriate or offensive messages such as racial, sexual, or religious slurs or jokes and sexually explicit messages or images, cartoons or jokes are prohibited.

7.2. Staff, or any person with access to PPN email(s) or social media, are not to use communal email systems to disseminate non-PPN-related information, except with the prior approval of the Secretariat.

7.3. Staff, or any person with access to PPN email(s) or social media, must not make derogatory comments regarding gender, marital status, family status, sexual orientation, religion, age, disability, race or membership of the Travelling community.

7.4. The Internet and social media must be used in a way that complies with current legislation, is acceptable to and does not create unnecessary risk to the PPN. In particular, the following is considered unacceptable:

7.4.1. visiting Internet sites that contain obscene, hateful, pornographic or otherwise illegal material

7.4.2. carrying out any form of fraud, or software, film or music piracy

7.4.3. using the Internet to send offensive or harassing material to other users

7.4.4. downloading commercial software or any copyrighted materials belonging to third parties, unless this download is permitted under a commercial agreement or other such licences

7.4.5. hacking into unauthorised areas

7.4.6. sending defamatory and/or knowingly false material, including about the PPN, its staff or volunteers

7.4.7. undertaking deliberate activities that waste staff effort or networked resources

7.4.8. introducing any form of malicious software into the organisation's network.

7.5 Social Media Posts

Appropriate posts would cover some or all of the following:

- Information on PPN events, news updates and elections
- Information on public consultations
- Information on funding opportunities from Cork County Council and others
- Press releases on the Department of Rural and Community Development activities
- Event information and occasional live coverage of events
- Important updates from Cork County Council and government departments
- Alerts about new content on the PPN website
- Practical information on services available through government departments
- Emergency updates (i.e. updates & advice relating to Covid-19 or weather warnings)
- Information about PPN Member Groups and their activities

Only posts from official sources relevant to the PPN should be shared/ retweeted e.g. the Council, DRCDG, government departments and agencies, local development companies, etc. Posts from PPN Member Groups may be shared or liked providing they are acceptable (see 7.4 above) and comply with this policy.

All posts and 'shared posts' should reflect the values and vision of the PPN.

If in any doubt, posts should not be posted/ shared.

8. Monitoring of Email and Internet Systems

8.1. The PPN will not at any time access private email accounts.

8.2. Monitoring of sites accessed on PPN or Council computers may be undertaken by the PPN or the Council to ensure adherence to this Policy or other relevant policies.

8.3. Records of Internet sites visited may be referred to where a breach of this Policy or other PPN policies is suspected. If illegal activity is suspected in relation to private email use the Gardaí will be contacted, in certain circumstances they will be entitled to access private email.

8.4. The Secretariat and the Council may access work email accounts and emails. If this occurs, staff will be informed prior to the accessing of email correspondence *if possible*. In relation to the privacy of emails received from people not in the organisation, all content will be treated confidentially.

The PPN email and website is part of the domain hosted by the Council., therefore this policy is intended to be in accordance with that of the Council.

8.5. Cork County Council may use software to monitor any inappropriate websites visited. Staff will be made aware if any misuse of PPN or Council technology is detected.

9. Sanctions

Where it is believed that staff, or any person with access to PPN email(s), have failed to comply with this policy, disciplinary action will be taken.

10. Privacy for PPN staff in the Workplace

10.1. Staff in Ireland have a right to a certain degree of privacy in the workplace. However, their right to privacy must be balanced with the legitimate rights and interests of their employer.

10.2 Cork County Council, as the employer, is required to put in place appropriate technical and organisational measures to ensure that any personal data it holds is secure and safe from outside intrusion.

11. Social Media

11.1 The PPN does not discriminate against staff or volunteers who use social media sites (Facebook, twitter etc.) for personal use on their own time. However:

11.1.1. bloggers are personally responsible for their commentary.

11.1.2. staff cannot use the Internet to harass, threaten, discriminate against, or disparage other employees or anyone associated with the PPN. Negative statements about the PPN, its services, its staff, PPN Member Groups, PPN representatives, Secretariat members team members, or any other related entity may lead to disciplinary action

11.1.3. staff cannot post photographs or videos of other staff members or volunteers, without their expressed consent

11.1.4. staff cannot write anything that breaches confidentiality, or negatively reflects on the PPN

11.2. Staff may use all social media platforms approved by the Secretariat but must at all times comply with this policy, GDPR requirements and all engagements must be respectful.

11.3. Staff must conduct social media exchanges with the same level of professionalism that they would conduct a face-to-face conversation. Staff should also be aware that comments left can be viewed by others, and therefore that they should be careful about sharing any information which should be kept confidential.

11.4 In the event that unacceptable feedback, engagement or mention of the PPN is received on social media, staff must not engage in any exchange with the author(s). Unacceptable material received in comments on the PPN's own platforms should be removed. The matter should be raised and discussed with the Secretariat and advice sought on how to limit any damage that may result.

11.5 If the organisation uses video clips on a media format such as YouTube, permission for their use must be received from all people who are featured. Where permission is withheld, the clip may not be used.

11.6 Staff members' personal social media profiles may state that they are involved with the PPN. In this regard, staff are asked to avoid any confusion by stating that:

- they are not representing the PPN in any official capacity
- all views, comments and opinions are strictly personal (i.e. the staff member's own, not those of the PPN)

Date approved by Plenary:

23/04/2026
