Cork County PPN Email and Internet Usage Policy

1. Introduction

Cork County PPN is committed to ensuring internet, email and fax usage that protects the organisation and its interests, and ensures requirements are met concerning dignity at work for all employees, and the protection of the individual's right to privacy.

2. Purpose

2.1. To ensure that Cork County PPN has clear policies outlining its internet and email usage.

2.2. To set out practical guidelines for transferring person-identifiable information (information which could be used to establish the identity of an individual).

2.3. To outline procedures in relation to social networking.

3. Scope

This policy applies to all email, internet and social media usage through the organisations email and internet system or on any work hardware being used in or out of work premises. It applies to all staff and visitors within the organisation. It also includes people from other agencies conducting in reach services in Cork County Council Offices for the time they are on the premises.

4. Email and Internet Use and Social Media Channels

4.1. The email system is to be used solely for the purposes of Cork County PPN and not for personal purposes of the employees.

4.2. Employees are permitted to use the internet for personal purposes during lunch breaks (or for duration of time e.g. 30 minutes per day). However, the limits of internet use outlined in this policy must be clearly followed, as employees will be using Cork County Council internet and will have to abide by the Council's Internet policies at all times.)

4.3. Where an employer has allowed the use of the company's communications facilities for private use by employees, such private communications may be subject to some surveillance, for example, to ensure adequate virus checking.

5. Sending Emails

5.1. E-mail is effectively on official headed paper and can be traced back to place, date and time of sending. Staff 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 are not to instigate or forward "unofficial mail" to users either within or outside the office which may be offensive or disruptive to others or which 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. Do not open any files that look suspicious or are from an unknown sender.

6.2. Should you receive material which you find offensive or abusive or time-wasting respond to it just as you would an offensive letter: complain directly to the sender and bring it to the attention of the sender's employing organisation in an appropriate way.

6.3. In the case of any Spam mail do not issue any reply.

7. Security

7.1. Do not leave your computer without securing the session by password or signing off.

7.2. If you think someone knows your password, ask for it to be changed as soon as possible. Maintaining the privacy of your password is your responsibility and consequently you are responsible for any abuses taking place using your name and password.

8. Inappropriate Email and Internet Use

8.1. 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 are prohibited. Sexually explicit messages or images, cartoons or jokes are prohibited.

8.2. Staff are not to use communal email systems to disseminate non work related information, except with the prior approval of management

8.3. Staff are not to make derogatory comments regarding gender, marital status, family status, sexual orientation, religion, age, disability, race or membership of the travelling community.

8.4. Internet must be used in a way that complies with current legislation, is deemed acceptable to the organisation, and does not create unnecessary risk to the organisation. In particular the following is deemed unacceptable use or behaviour by employees:

8.4.1. visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material

8.4.2. using the computer to perpetrate any form of fraud, or software, film or music piracy

8.4.3. using the internet to send offensive or harassing material to other users

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

8.4.5. hacking into unauthorised areas

8.4.6. sending defamatory and/or knowingly false material about Cork County PPN

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

8.4.8. introducing any form of malicious software into the organisations network.

8.5 Social Media Posts

Appropriate posts would cover some or all of the following:

- Information on Cork County PPN events, news updates and elections,
- Information on public consultations,
- Information on funding opportunities form 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 form 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).

Only posts from official sources relevant to the Cork County PPN should be shared/ retweeted e.g.Cork County Council, Department of Rural and Community Development, government departments and agencies, local development companies, etc.

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

If in any doubt, do not post/ share.

9. Monitoring of Email and Internet Systems

9.1. The organisation cannot at any time access private email accounts.

9.2. Monitoring of sites accessed on work computers may be undertaken by the organisation to ensure adherence to the internet and email policy or other relevant organisational policies.

9.3. Records of which sites have been accessed may be referred to if required in a situation of suspected breech of internet usage policy. If any illegal activity is suspected in relation to private email usage the Gardaí will be contacted, in certain circumstances the Gardaí will be entitled to access private email.

9.4. The Secretariat and County Council may access work email accounts and emails. In this instance staff will be informed prior to the accessing of email correspondence if at all 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 Cork Co Co., therefore this policy is intended to be in accordance with that of Cork County Council.

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

10. Sanctions

10.1. Where it is believed that an employee has failed to comply with this policy, disciplinary actions will be implemented.

11. Privacy in the Workplace

11.1. Employees in the workplace in Ireland have a legitimate 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 the employer.

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

12. Social Media

12.1 Cork County PPN does not discriminate against employees who use social media sites (Facebook, twitter etc.) for personal use on their own time. However:

12.1.1. Bloggers are personally responsible for their commentary.

12.1.2. Staff cannot use the Internet to harass, threaten, discriminate against, or disparage other employees or anyone associated with Cork County PPN. Negative statements about Cork County PPN its services, its team members, or any other related entity may lead to disciplinary action.

12.1.3. Staff cannot post photographs or videos of other team members without express written consent and authorisation from management.

12.1.4. Staff cannot write anything that conflicts with any areas of confidentiality, or negatively reflects on the professionalism of the organisation.

12.2. Staff should not use social media such as Facebook and twitter unless this is a stated part of a PPN programme.

12.3. If social media is permitted as part of a programme, staff should take care to conduct 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 any information they may wish to keep confidential.

12.4. If the organisation uses video clips on a media format such as YouTube, it is important that permission has been received.

12.5 Your personal social media profile may state that you are involved with the PPN. In this regard, you must avoid any confusion by stating that:
• You are not representing the PPN in any official capacity.
• All views, comments and opinions are strictly personal (i.e. your own and not those of the PPN)
• All views, comments and opinions are in no way associated with the PPN

Date approved by Plenary: