Ashington Parish Council
IT Security Policy – staff
October 2022

IT, Communications and Monitoring

Ashington Parish Council (APC) provides employees with access to various computer facilities for work and communication purposes. In order to ensure compliance with all applicable laws in relation to data protection, information security and compliance monitoring, APC has adopted an IT communications and monitoring policy which should be read in conjunction with its' Data Protection policy.

Breach of the policy

Breach of this policy will be regarded as a disciplinary offence and will be dealt with under the Council's formal disciplinary process.

Anyone who considers that there has been a breach of this policy in relation to personal information about them held by the Council should raise the matter via the Council's formal grievance procedure.

IT, communications and monitoring

APC makes use of IT systems, for data storage, communications and as a source of information. We have adopted an IT, communications and monitoring policy in order to:

- prevent inappropriate use of computer equipment (such as extended personal use or for accessing and circulating pornographic, racist, sexist or defamatory material);
- protect confidential, personal or commercially sensitive data;
- prevent the introduction of viruses;
- prevent the use of unlicensed software;
- ensure that Council property is properly looked after; and
- monitor the use of computer facilities to ensure compliance with internal policies and rules and to detect abuse.

IT, communication and monitoring policy ("the policy")

Introduction

1. APC provides you with access to various computing, telephone and postage facilities ("the Facilities") to allow you to undertake the responsibilities of your position and to improve internal and external communication.

2. This policy sets out the Council's position on your use of the Facilities and it includes:

    - your responsibilities and potential liability when using the Facilities
    - the monitoring policies adopted by the Council; and
    - guidance on how to use the Facilities.

3. This policy has been created to:

    - ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring
    - protect the Council from the risk of financial loss, loss of reputation or libel; and
    - ensure that the Facilities are not used so as to cause harm or damage to any person or organisation.

4. This policy applies to the use of:

    - local, inter-office, national and international, private or public networks and all systems and services accessed through those networks;
    - desktop, portable and mobile computers and applications;
    - social media; and
    - electronic mail and messaging services.

Computer facilities: Use of computer systems

5. Subject to anything to the contrary in this policy the Facilities must be used for Council business purposes only.

6. In order to maintain the confidentiality of information held on or transferred via the Council's Facilities, security measures are in place and must be followed at all times. A log-on ID and password is required for access to the Council's equipment/network. This will be changed regularly and must be kept secure and not shared with anyone.

7. You are expressly prohibited from using the Facilities for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Council or its clients other than in the normal and proper course of carrying out your duties for the Council.

8. In order to ensure proper use of Council computers, you must adhere to the following practices:

    - anti-virus software must be kept running at all times;

    - media storage such as USB drives, CD's or portable hard drives will not be permitted unless they have been provided by the IT supplier or approved by Council;

    - obvious passwords such as birthdays and spouse names, etc, must be avoided (the most secure passwords are random combinations of letters and numbers);

    - all files must be stored on the network/computer hard drive which is backed up regularly to avoid loss of information; and

    - always log off the computer/network before leaving your computer for long periods of time or overnight.

Software

9. Software piracy could expose both the Council and the user to allegations of intellectual property infringement. The Council is committed to following the terms of all software licences to which the Council is a contracting party. This means, in particular, that:

    - software must not be installed onto any of the Council's computers unless this has been approved in advance by our IT Contractors or Council. They will be responsible for establishing that the appropriate licence has been obtained, that the software is virus free and compatible with the computer Facilities; and
    - software should not be removed from any computer nor should it be copied or loaded on to any computer without prior consent.

Laptop computers, PC's, tablets and smart phones

10. Laptop computers, PC's, tablets and smart phones belonging to the Council along with related equipment and software are subject to all of the Council's policies and guidelines governing non-portable computers and software). All laptops, PC's and tablets will be encrypted. When using such equipment:

    - you are responsible for all equipment and software until you return it. It must be kept secure at all times;

    - you are the only person authorised to use the equipment and software issued to you;

    - you must work within the Councils filing/software environment when carrying out Council business to ensure that all data is backed up and accessible by the Clerk;

    - if you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the Council's attention;

    - upon the request of the Council at any time, for any reason, you will immediately return any equipment and all software to the Council; and

    - if you are using your own laptop or PC to connect with the Council's network or to transfer data between the laptop or PC and any of the Council's computers you must ensure that you have obtained prior consent, comply with instructions and ensure that any data downloaded or uploaded is free from viruses.

Email (internal or external use)

11. All staff will be issued a Council email account which should be used when transacting on behalf of the PC.

12. Internet email is not a secure medium of communication; it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If you are sending confidential information by email this should be sent using password protected attachments.

13. Email should be treated as any other documentation. If you would normally retain a certain document in hard copy you should retain the email.

14. Do not forward email messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo with the same information do not forward the email.

15. Your email inbox should be checked on a regular basis.

16. As with many other records, email may be subject to discovery in litigation. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

17. Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of the Facilities is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

18. Staff will be required to surrender their email account and all of its contents to the Clerk if they decide to leave the Council.

Internet

19. Posting information on the internet, whether on a newsgroup, via a chat room or via email is no different from publishing information in the newspaper. Staff should confirm the posting with the Clerk prior to issue.

20. Using the internet for the purpose of trading or carrying out any business activity other than Council business is strictly prohibited.

21. For the avoidance of doubt the matters set out above include use of wireless facilities.

Monitoring policy

22. The policy of the Council is that we may monitor your use of the Facilities.

23. The Council recognises the importance of an individual's privacy but needs to balance this against the requirement to protect others and preserve the integrity and functionality of the Facilities.

24. The Council may from time to time monitor the Facilities. Principal reasons for this are to:

    - detect any harassment or inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex discrimination policies;

    - ensure compliance of this policy;

    - detect and enforce the integrity of the Facilities and any sensitive or confidential information belonging to or under the control of the Council;

    - ensure compliance by users of the Facilities with all applicable laws (including data protection), regulations and guidelines published and in force from time to time; and

    - monitor and protect the wellbeing of employees.

25. The Council may adopt at any time a number of methods to monitor use of the Facilities. These may include:

    - recording and logging of internal, inter-office and external telephone calls made or received by employees using its telephone network (including where possible mobile telephones). Such recording may include details of length, date and content;

    - recording and logging the activities by individual users of the Facilities. This may include opening emails and their attachments, monitoring Internet usage including time spent on the internet and websites visited;

    - physical inspections of individual users computers, software and telephone messaging services;

    - periodic monitoring of the Facilities through third party software including real time inspections;

    - physical inspection of an individual's post; and

    - archiving of any information obtained from the above including emails, telephone call logs and Internet downloads.

26. The Council will not (unless required by law):

    - allow third parties to monitor the Facilities (with the exception of our appointed IT supplier); or
    - disclose information obtained by such monitoring of the Facilities to third parties unless the law permits.

27. The Council may be prohibited by law from notifying employees using the Facilities of a disclosure to third parties.

Social Media

28. The Council may use social media to communicate messages to residents and will only be used:

    - by the Clerk and persons nominated by the Clerk;
    - to transmit factual information and news, not personal opinion;
    - to respond to comments and requests submitted via the account.

29. Staff using their own social media accounts must ensure that any comment made is clearly identified as their own and not representative of the Council.

General guidance

30. Never leave any equipment or data (including client files, laptops, computer equipment and mobile phones) unattended on public transport or in an unattended vehicle.

31. When using email or sending any form of written correspondence:

- be careful what you write; never forget that email and written correspondence are not the same as conversation: they are a written record and can be duplicated at will;

- use normal capitalisation and punctuation; typing a message all in capital letters is the equivalent of shouting at the reader;

- check your grammar and spelling; and

- do not forget that emails and other forms of correspondence should maintain the high standards expected by the Council.

Observation of this policy is mandatory and forms part of the terms and conditions of employment of staff and the terms of access to Ashington Parish Council's systems and offices. **Misuse of the Facilities will be treated as gross misconduct and may lead to dismissal.**