



## **IT and COMMUNICATIONS POLICY**

**2018**

### **INTRODUCTION**

Information Technology (IT) and Communications play an essential role in the conduct of our Council business. The IT infrastructure including e-mail and internet access have significantly improved business operations and efficiencies.

How you communicate with people not only reflects on you as an individual but also on us as a Council. As a result of this the Council values your ability to communicate with colleagues, clients/customers and business contacts but we must also ensure that such systems and access are managed correctly, not abused in how these are used or what they are used for,

This policy applies to all members of Finchampstead Parish Council (FPC) who use our communications facilities, whether full or part-time employees, contract staff, temporary staff or councillors. The parameters and restrictions are outlined below and you are required to read them carefully.

### **GENERAL PRINCIPLES**

You must use our IT and communications facilities sensibly, professionally, lawfully, consistently with your duties and in accordance with this policy and other Council rules and procedures.

At all times employees and councillors must behave with honesty and integrity and respect the rights and privacy of others in relation to electronic communication and information. The Council reserves the right to maintain all electronic communication and files.

Every employee will be given access to the Internet as appropriate to their job needs.

All PC/network access will be through passwords. Employees are not permitted to share their password with anyone inside or outside the Council. Individuals will be allowed to set their own passwords, and must change them as frequently as requested by the system set-up requirements.

All information relating to our clients/customers and our Council operations both paper-based and electronic information must be treated with utmost care and remain confidential where necessary.

Many aspects of communication are protected by intellectual property rights which can be infringed in a number of ways. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

Particular care must be taken when using e-mail as a means of communication because all expressions of fact, intention and opinion in an e-mail may bind you and/or the Council and can be produced in court in the same way as other kinds of written statements.

If you are speaking with someone face to face, via the telephone, or in writing via whatever medium you are a representative of the Council. Whilst in this role you should not express any personal opinion that you know or suspect might be contrary to the opinions of the Council and its policy.



## **USE OF ELECTRONIC MAIL**

### **Business use**

FPC provides email addresses for the use of councillors and staff. It does not provide computer equipment but will consider requests by councillors for assistance in training in use of new technology.

All staff and councillors must use the provided FPC email addresses for conducting FPC business. These email facilities will be withdrawn when the employee or councillor leaves the council.

All FPC email will contain this standard email disclaimer:

The contents of this message and any attachments to it are confidential and may be legally privileged. If you have received this message in error, you should delete it from your system immediately and advise the sender.

To any recipient of this message within Finchampstead Parish Council, unless otherwise stated you should consider any personal information contained in this message and attachments as confidential.

Finchampstead Parish Council is a public authority and most personal data is processed for compliance with a legal obligation or statutory duty. Where there is no legal or statutory duty we rely on the consent from the individual. Your personal data is held in accordance with our privacy notice which can be viewed on our website [www.finchampstead-pc.gov.uk](http://www.finchampstead-pc.gov.uk) and which is kept under regular review.

Local Council legislation and FPC procedures do not allow for electronic decision-making. Expressly, email exchanges should not be used for any decision making (or discussions about topics) pertaining to the remit of main council or committees. Exceptions to this must be by formal recorded agreement at the appropriate governing meeting or forum.

All correspondence is subject to formal scrutiny, and FPC requires email to conform to the same level of scrutiny as all other means of communication. Therefore, when using email, councillors and staff will conform to codes of conduct and such procedural and legal constraints as apply to all other activities.

Always use the "Bcc" box when mailing to groups whenever the members of the group are unaware of the identity of all the others (as in the case of marketing mailing lists), or where you judge that the membership of the group of one or more individuals should perhaps not be disclosed to the others (as in the case of members of a staff benefit scheme), because if you use the "Cc" box each recipient is informed of the identity (and in the case of external recipients, the address) of all the others. Such a disclosure may breach any duty of confidence owed to each recipient, breach the Council's obligations under the General Data Protection Regulation and Data Protection Acts or may inadvertently disclose confidential Council information such as contact list. This applies to both external and internal e-mail.

Expressly agree with the customer/client that the use of e-mail is an acceptable form of communication bearing in mind that if the material is confidential, privileged or commercially sensitive then un-encrypted e-mail is not secure.

If you have sent an important document, always telephone to confirm that the e-mail has been received and read.

In light of the security risks inherent in web-based e-mail accounts, you must not e-mail business documents to your personal web-based accounts. You may send documents to a customer's/client's web-based account if you have the customer's/client's express written permission to do so. However, under no circumstances should you send sensitive or highly confidential documents to a customer's/client's personal web-based e-mail account (e.g. Yahoo, or Hotmail), even if the customer/client asks you to do so.



### Personal use

- a) Although our e-mail facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on condition that all the procedures and rules set out in this policy are complied with. Be aware, however, that if you choose to make use of our facilities for personal correspondence, the Council may need to monitor communications for the reasons shown below.
- b) Under no circumstances may the Council's facilities be used in connection with the operation or management of any business other than that of the Council unless express permission has been obtained from the Clerk.
- c) You must ensure that your personal e-mail use:
  - does not interfere with the performance of your duties
  - does not take priority over your work responsibilities
  - does not cause unwarranted expense or liability to be incurred by the Council or our clients
  - does not have a negative impact on our business in any way
  - is lawful and complies with this policy.
- d) The Council will not tolerate the use of the E-mail system for unofficial or inappropriate purposes, including:
  - any messages that could constitute bullying, harassment or other detriment;
  - on-line gambling
  - accessing or transmitting pornography
  - transmitting copyright information and/or any software available to the user
  - posting confidential information about other employees, the Council or its customers or suppliers.



## **USE OF INTERNET**

We trust you to use the internet sensibly. Although internet facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own personal purposes. This is permitted on condition that all the procedures and rules set out in this policy are complied with and your use of the internet does not interfere in any way with the performance of your duties.

Whenever you access a web site, you should always comply with the terms and conditions governing its use. Care must be taken in the use of information accessed through the Internet. Most information is unregulated, and as such there is no guarantee of accuracy.

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.

You must not:

- use any images, text or material which are copyright-protected, other than in accordance with the terms of the license under which you were permitted to download them
- introduce packet-sniffing or password-detecting software
- seek to gain access to restricted areas of the Council's network
- access or try to access data which you know or ought to know is confidential
- introduce any form of computer virus
- carry out any hacking activities.

## **VIRUS PROTECTION PROCEDURES**

In order to prevent the introduction of virus contamination into the software system the following must be observed:-

- unauthorised software including public domain software, magazine cover disks/CDs or Internet/World Wide Web downloads must not be used
- all software must be virus checked using standard testing procedures before being used.

## **USE OF COMPUTER EQUIPMENT**

In order to control the use of the Council's computer equipment and reduce the risk of contamination the following will apply.

- The introduction of new software must first of all be checked and authorised by the Clerk and a nominated Councillor before general use will be permitted.
- Only authorised staff should have access to the Council's computer equipment.
- Only authorised software may be used on any of the Council's computer equipment.
- Only software that is used for business applications may be used.
- No software may be brought onto or taken from the Council's premises without prior authorisation.
- Unauthorised access to the computer facility will result in disciplinary action.
- Unauthorised copying and/or removal of computer equipment/software will result in disciplinary action, such actions could lead to dismissal.



## **SYSTEM SECURITY**

Security of our IT systems is of paramount importance. We owe a duty of care to all of our customers/clients to ensure that all of our business transactions are kept confidential where appropriate. If at any time we need to rely in court on any information which has been stored or processed using our IT systems it is essential that we are able to demonstrate the integrity of those systems. Every time you use the system you take responsibility for the security implications of what you are doing.

The Council's system or equipment must not be used in any way which may cause damage, or overloading or which may affect its performance or that of the internal or external network.

Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorised third party.

## **WORKING REMOTELY**

This part of the policy and the procedures in it apply to your use of our systems, to your use of our laptops, and also to your use of your own computer equipment or other computer equipment whenever you are working on Council business away from our premises (working remotely).

When you are working remotely you must:

- password protect any work which relates to our business so that no other person can access your work;
- position yourself so that your work cannot be overlooked by any other person;
- take reasonable precautions to safeguard the security of our laptop computers and any computer equipment on which you do Council business, and keep your passwords secret;
- inform the police and the Council as soon as possible if either a Council laptop in your possession or any computer equipment on which you do our work has been stolen; and
- ensure that any work which you do remotely is saved on the Council system or is transferred to our system as soon as reasonably practicable.

PDA's or similar hand-held devices and memory sticks are easily stolen and not very secure so you must password-protect access to any such devices used by you on which is stored any personal data of which the Council is a data controller or any information relating to our business.

## **PERSONAL TELEPHONE CALLS/ MOBILE PHONES**

Telephones are essential for our business. Incoming/outgoing personal telephone calls are allowed at the Council's premises but should be kept to a minimum. We reserve the right to recharge for excessive personal use.

Personal mobile phones should be used only when necessary during working hours.



## **MONITORING OF COMMUNICATIONS BY THE COUNCIL**

The Council is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy. The Council may monitor your business communications for reasons which include:

- providing evidence of business transactions;
- ensuring that our business procedures, policies and contracts with staff are adhered to;
- complying with any legal obligations;
- monitoring standards of service, staff performance, and for staff training;
- preventing or detecting unauthorised use of our communications systems or criminal activities; and
- maintaining the effective operation of Council communication systems.

From time to time the Council may monitor telephone, e-mail and internet traffic data (i.e. sender, receiver, subject; non-business attachments to e-mail, numbers called and duration of calls; domain names of web sites visited, duration of visits, and non-business files downloaded from the internet) at a network level (but covering both personal and business communications). 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.

Sometimes it is necessary for us to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday.

## **DATA PROTECTION**

As an employee or councillor using our communications facilities, you will inevitably be involved in processing personal data for the Council as part of your role. Data protection is about the privacy of individuals, and is governed by the General Data Protection Regulation and current Data Protection Acts.

Whenever and wherever you are processing personal data for the Council you must keep this confidential and secure, and you must take particular care not to disclose such data to any other person (whether inside or outside the Council) unless authorised to do so. Do not use any such personal data except as authorised by us for the purposes of your role. If in doubt ask the Clerk.

The Acts give every individual the right to see all the information which any data controller holds about them. Bear this in mind when recording personal opinions about someone, whether in an e-mail or otherwise. It is another reason why personal remarks and opinions made should be given responsibly, must be relevant and appropriate as well as accurate and justifiable.

For your information, the Act provides that it is a criminal offence to obtain or disclose personal data without the consent of the data controller. "Obtaining" here includes the gathering of personal data by employees at work without the authorisation of the employer. You may be committing this offence if without authority of the Council: you exceed your authority in collecting personal data; you access personal data held by us; or you pass them on to someone else (whether inside or outside the Council).



## **USE OF SOCIAL NETWORKING SITES OR SOCIAL MEDIAS**

Social media can be categorised into six types – blogs, wikis, social networks, forums, podcasts and content communities. Popular packages include Twitter, Facebook, You Tube, Pinterest, Myspace, LinkedIn, Whatsapp and Instagram, each with a different focus – sharing, conversation, relationships, groups and reputation. The key feature of such systems is that they can be accessed in different ways – via computers, tablets and mobile ‘phones.

The Council uses Facebook to disseminate information on Council activities, official releases of public information from trusted sources, and community events and activities potentially of interest to/ available to all residents.

The Clerk is the designated owner of and is responsible for the management of the Facebook account. All of the Council’s communications via its Facebook Page are managed by the Clerk and Assistant to the Clerk.

The Council uses Whatsapp as a communication tool between Council staff and councillors only.

Any work related issue or material that could identify an individual who is a customer/client or work colleague, which could adversely affect the Council a customer/client or our relationship with any customer/client must not be placed on a social networking site.

## **CONFIDENTIALITY**

Employees are not permitted to register with sites or electronic services in the Council’s name without the prior permission of the Clerk or nominated councillor. They are not permitted to reveal internal Council information to any sites, be it confidential or otherwise, or comment on company matters, even if this is after-hours or personal use. This applies to all electronic communication and data.

## **COMPLIANCE WITH THIS POLICY**

Failure to comply with this policy may result in disciplinary action being taken against you. If there is anything in this policy that you do not understand, please discuss it with the Clerk.

Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time.

DATE OF ADOPTION: 17/10/2018

REVIEW DATE: 17/01/2019

