



IT, Communications and Monitoring Policy

Background

1. Birdham Parish Council (BPC) provides its employee/councillors with access to various computer facilities for work and communication purposes. To ensure compliance with all applicable laws in relation to data protection, information security and compliance monitoring, Birdham Parish Council has adopted an IT communications and monitoring policy which should be read in conjunction with its Data Protection policy.
2. BPC makes use of IT systems, for data storage, communications and as a source of information. BPC has adopted an IT, communications, and monitoring policy 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.

THE POLICY

Introduction

3. BPC provides you with access to various computing facilities (“the Facilities”) to allow you to undertake the responsibilities of your position and to improve internal and external communication.
4. This policy sets out BPC’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 BPC; and
 - guidance on how to use the Facilities.

5. This policy has been created to:

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

6. This policy applies to the use of:

- local, 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 laptops

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

8. To maintain the confidentiality of information held on or transferred via BPC'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 BPC's laptops. This will be changed regularly and must be kept secure and not shared with anyone.

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

10. To ensure proper use of BPC 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.
- 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 an external drive which is backed up regularly to avoid loss of information; and

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

Software

11. Software piracy could expose both BPC and the user to allegations of intellectual property infringement. BPC is committed to following the terms of all software licences to which BPC is a contracting party. This means that:

- software must not be installed onto any of BPC's computers unless this has been approved in advance by our IT Contractors. 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 smartphones

12. Laptop computers, PC's, tablets, and smartphones belonging to BPC along with related equipment and software are subject to all of BPC'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 Sharepoint environment when carrying out BPC business to ensure that all data is backed up and accessible by admin staff.
- if you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to BPC's attention.
- upon the request of BPC at any time, for any reason, you will immediately return any equipment and all software to BPC; and
- if you are using your own laptop or PC to connect with BPC's network or to transfer data between the laptop or PC and any of BPC'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)

13. All staff and councillors are issued with a .gov.uk email account which must be used when transacting on behalf of BPC.
14. 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. Do not send attachments containing personal data, always use a link from the SharePoint.
15. Email should be treated as any other documentation. If you would normally retain a certain document in hard copy, you should retain the email.
16. 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.
17. Your email inbox should be checked on a regular basis.
18. 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. 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.
19. Councillors will be required to surrender their email account and all its contents to the Clerk if they decide to leave BPC.

Internet

20. 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. Councillors should confirm the posting with the Clerk prior to issue.
21. Using the internet for the purpose of trading or carrying out any business activity other than BPC business is strictly prohibited.
22. For the avoidance of doubt the matters set out above include use of wireless facilities.

Monitoring policy

23. The policy of BPC is that it may monitor your use of the Facilities.

24. BPC 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.
25. BPC may from time to time monitor the Facilities. Principal reasons for this are to:
- detect any harassment or inappropriate behaviour by councillors, ensuring compliance with relevant policies including 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 BPC.
 - 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 councillors.
26. BPC may adopt at any time several methods to monitor use of the Facilities. These may include:
- opening emails and their attachments;
 - physical inspections of individual users' computers, and software
 - periodic monitoring of the Facilities through third party software including real time inspections.
 - archiving of any information obtained from the above including emails, telephone call logs and Internet downloads.
27. BPC will not (unless required by law):
- allow third parties to monitor the Facilities (except for our appointed IT supplier); or
 - disclose information obtained by such monitoring of the Facilities to third parties unless the law permits.
28. BPC may be prohibited by law from notifying councillors using the Facilities of a disclosure to third parties.

Social Media

29. BPC may use social media to communicate messages and will only be used:
- by the clerk and any councillor nominated at a meeting.
 - to transmit factual information and news, not personal opinion.

- to respond to comments and requests submitted via the account.
30. Staff using their own social media accounts must ensure that any comment made is clearly identified as their own and not representative of BPC.

General guidance

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

Breach of the policy

33. Observation of this policy is mandatory and forms part of the terms and conditions of being a councillor and the terms of access to BPC's systems.
34. Breach of this policy will be regarded as a disciplinary offence and will be dealt with under BPC's formal disciplinary process.
35. Anyone who considers that there has been a breach of this policy in relation to personal information about them held by BPC should raise the matter via BPC's formal grievance procedure.

Signed: _____ Date: _____

Councillor Signature