|  |  |
| --- | --- |
| PCC LOGO | IT Policy |

Document Overview

|  |  |
| --- | --- |
| **Purpose** | The purpose of this policy is to ensure that staff understand the rules surrounding IT, Software, Emails and Internet use. This policy applies to all permanent and temporary staff, and contractors on site or using Company equipment. |
| **Confidentiality** | This document is not confidential. |
| **Document owner** |  |
| **Status note** | Draft/Final |
| **Distribution** | All PCC staff. |
| **Required action** |  |
| **Proposed next step** |  |

Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Status Note** |
| 1 | 05.06.2023 | HR Template |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. Use of IT Equipment
	1. In order to control the use of IT equipment and protect the integrity of the Company’s data, the following will apply:
	2. The introduction of new software must first of all be checked and authorised by the Systems Manager before use will be permitted.
	3. Only authorised staff may have access to the IT equipment. All operational procedures must be adhered to at all times.
	4. Only authorised software may be used on any of the IT equipment. Only software that is used for relevant business applications may be used.
	5. No software may be taken from the Company’s premises without prior authorisation.
	6. Unauthorised access of the computer facility will result in disciplinary action. Unauthorised copying, alteration or removal of programs or data will result in disciplinary action. Such actions could lead to dismissal.
	7. All employees must not disclose their passwords to anyone else.
	8. Please note that the above section refers to all equipment purchased through the relevant budget headings and housed in any of the Parish buildings or offices.
	9. The Company reserves the right to carry out regular monitoring of Employees’ use of all Company computer equipment including the e-mail system, particularly in cases where it is suspected that some form of system or equipment abuse may be happening or where other unacceptable practices are taking place.
2. Internet

**Policy**

* 1. The use of the Internet within the Company is encouraged, as its appropriate use provides access to a wide range of useful information. Used correctly, it is a facility which can be of valuable assistance to the Company and to employees in the performance of their jobs. Its inappropriate use, however, causes many problems, ranging from excessive costs for the Company to possible legal claims against the Company.

**Monitoring**

* 1. The Company reserves the absolute right to monitor employees' use of the Internet.

Authorised Use

* 1. Access to the Internet is provided to employees for matters directly concerned with the business of the Company.
	2. You may only use the Company’s internet system for personal use during your breaks.
	3. You should be aware that:
		1. Leaving Internet access open while away from your desk means that unauthorised use may occur during the absence and be attributable to you and therefore you are required to lock your workstation whenever you are away from your desk
		2. Your use of the internet will be monitored and logged.

**Unauthorised Use**

* 1. The Company will not tolerate the use of the Internet for any of the following:
		1. Accessing/downloading pornography or other illegal or obscene material.
		2. Downloading software which has not been virus checked and approved.
		3. Personal communication e.g. chatrooms and social media (see below)
		4. Accessing on-line personal services without authorisation such as holidays, shopping, banking, gambling.
		5. Creating and/or operating a personal web site or blogging during work time, unless it is a work related blog.
		6. This is not an exhaustive list.
	2. Social Media: all staff must abide by the Company’s rules relating to use of social media as set out in the Social Media Policy. (Appendix 10).

**Computer Software**

* 1. Because of potential virus infection and consequent damage to the business, you must not load any software into any computer via any source, including memory sticks, flash drives, pen drives, or any portable memory devices, without the prior approval of management. Such approval will only be given after virus checking.
	2. Virus protection software is maintained and periodically updated.
	3. Under no circumstances must you load games or free issue software onto Company equipment.
	4. If a specific application programme is necessary for your work, then it will be purchased by the Company for your use.
	5. You must not make 'pirate' copies of Company owned software for use by other persons either inside or outside the Company. This not only breaks Company rules, it is an illegal practice.
	6. **Failure to comply with any procedure relating to internet and computer software use may result in a disciplinary warning or dismissal, depending on the circumstances.**
1. Emails

**Policy**

* 1. The use of the e-mail system within the Company is encouraged, as its appropriate use facilitates communication and improves efficiency. Used correctly, it is a facility that is of assistance to many employees. Its inappropriate use, however, causes many problems ranging from minor distractions to legal claims against the Company. This section sets out the Company's view on the correct use of the e-mail system, and explains how this can be achieved, as well as the Company's responses to inappropriate use.

**Authorised Use**

* 1. The e-mail system is available for communication on matters directly concerned with the business of this Company. Employees using the e-mail system should give particular attention to the following:
	2. The style and content of an e-mail message must be consistent with the standards that the Company expects from written communications.
	3. e-mail messages should only be sent to those employees for whom they are particularly relevant.
	4. e-mail should not be used as a substitute for face to face communication; "Flame-mails" (e-mails that are abusive) can be a source of stress and can damage working relationships, while hasty messages, sent without proper consideration, can cause unnecessary misunderstandings.
	5. If an e-mail is confidential, the user must ensure that the necessary steps are taken to protect confidentiality.
	6. When sending emails to personal addresses ensure compliance with the Data Protection Policy and GDPR to avoid a data breach. All data breaches must be reported to the Director of Operations. (See Appendix 13).
	7. The Company will be liable for infringing copyright or any defamatory information circulated either within the Company or to external users of the system.
	8. Offers or contracts transmitted via e-mail are as legally binding on the Company as those sent on paper.
	9. Employees must keep up to date with emails in the same way as any other communication and ensure that their inbox is regularly attended to and that out of office notifications are used if the inbox is to be left unattended for any length of time exceeding one day. Failure to maintain an inbox in this way is likely to result in disciplinary action.

**Unauthorised use**

* 1. Unauthorised or inappropriate use of e-mail may result in disciplinary action.
	2. Although “inappropriate” is purposely not defined here, the Company reserves the right to determine when a contravention fits this description.
	3. Users should be aware that the Company reserves the right to access individual employee’s e-mail accounts in cases where, in the Company’s view, there is a legitimate business need to do so.
	4. In-house training in the use of e-mail will be provided as appropriate. Line Managers are required to ensure that all new employees receive the training they need prior to using the e-mail system.
	5. Critical information must not be stored solely within live or archived e-mails. Appropriate files should be stored elsewhere on the system. In most cases a paper copy does not need to be kept. If in doubt check with your Line Manager.
	6. Employees who have cause for complaint as a result of e-mail communications should raise the matter initially with their immediate Line Manager and/or the Systems Manager. If appropriate, the complaint can then be raised through the Company’s Grievance Procedure. (Appendix 5).
1. Electronic Files
	1. Unknown files or messages should never be introduced into the system without first being checked for viruses.
	2. Users are reminded that the mere deletion of a message or file may not fully eliminate it from the system.
	3. Users are required to be familiar with the requirements of the UK GDPR and Data Protection Act 2018 and to ensure that they operate in accordance with the requirements of the Act. Details are available from the Systems Manager.