group policies and procedures

# acceptable use policy

|  |  |
| --- | --- |
| Category | Corporate Governance  |
| Author | James Leyland |
| Responsible Director | James Leyland |
| Date of issue | November 2023 |
| Next review date | November 2025 |
| Document ref & version | Acceptable Use Policy V1 |

**Related policies and guidance**

**Document revision and approval history**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author | Approved by | Comments |
| V1 |  Nov 2023 |  JL | JL & FC |  |

# purpose & Scope

The purpose of this Policy is to ensure the acceptable use of all computer and information resources, including hardware, software, networks, internet access, emails, and other electronic communication systems, by staff, employed or subcontracted. The policy protects the integrity and confidentiality of the IT infrastructure, promoting responsible and ethical behaviour when using these systems and resources.

Staff and all other users must adhere to all policies and protocols in addition to this Acceptable Use Policy.

# policy

**Acceptable Use**

Staff must use IT infrastructure for all patient interactions (the patient record) to ensure contemporaneous, accurate patient notes as well as for the use of personal training, HR purposes, internal and external communications etc.

All users of the IT resources of Castleman Healthcare (the Company) or of GP practices must comply with all applicable laws, regulations, and policies, including but not limited to the Data Protection Act 2018, General Data Protection Regulation (GDPR), and any related data protection or confidentiality policies.

All users of the IT resources of the Company or those used by practices are responsible for maintaining the security of these resources by using strong passwords (with letters, numbers, characters etc.) updating software if advised to do so, and reporting any suspicious activity to Trusted Technology who maintain the system.

The Company respects the privacy of its employees and expects all users to respect the privacy of others. Any unauthorised access, use, or disclosure of personal information is strictly prohibited.

Users must comply with any request made to them by the Company or Trusted Technology in connection with the enforcement of these Regulations.

Users shall not use the IT infrastructure facilities inappropriately or illegally.

**Unacceptable Use**

Company and practice IT Systems may not be used directly or indirectly by a staff member for the download, creation, manipulation, transmission or storage of:

1. any offensive, obscene, pornographic/indecent material, data or other, or any data capable of being resolved into obscene or indecent images or material;
2. unlawful material or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
3. unsolicited and unauthorised “spam” emailing.
4. material which is subsequently used to facilitate harassment, bullying and/or victimisation.
5. material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
6. material with the intent to defraud or which is likely to deceive a third party;
7. material which advocates or promotes any unlawful act;
8. material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
9. material that brings the Company or the practices into disrepute.

IT systems must not be deliberately used by a User for activities having, or likely to have, any of the following characteristics:

1. Accessing or attempting to access unauthorised information or resources.
2. Sharing passwords or other access credentials with others.
3. Engaging in any activity that may disrupt or interfere with the normal operation of the Company or practice(s).
4. Commercial activities
5. Security breaches or compromise of IT systems.
6. Intentionally or recklessly introducing any form of spyware, computer virus or other potentially malicious software;
7. Installing or using unauthorised software or hardware.
8. Use software which is only licensed for limited purposes for other purpose or otherwise breaching software licensing agreements;
9. Fail to comply with a request from an authorised person for you to change your password.

Trusted Technology use an email system that is intended for activities pertaining to your role within the Company only.

All users of the email system should not harass, threaten, or intimidate others, solicit or promote personal or commercial activities, send confidential or sensitive information without using appropriate encryption methods.

Social media should not be used unless authorised to do so by one of the Directors and only then will the Director(s) monitor what is being posted before posting to ensure Social Media content is responsible and ethical manner.

The Company reserves the right to monitor all activities on its IT resources, including but not limited to email and internet usage, contemporaneous record keeping etc. Unauthorised use of IT resources may result in disciplinary action.

**Conserquences of Breach**

In the event of a breach of this Acceptable Use Policy by a User, the Company will;

1. Start an immediate investigation.
2. restrict or terminate a User’s right to use the IT Systems if deemed necessary.
3. withdraw or remove any material uploaded by that User in contravention of this policy;
4. disclose information to law enforcement agencies and/or the Information Commissioners Office and take the required legal action against the employee who breaching this policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.