POLICY H

IT POLICY

Policy Statement

This policy applies to the use of all computer equipment and software belonging to the Company. It also applies to all private systems, whether owned, leased, rented or on-loan, when connected to the Company's network directly or indirectly.

The IT systems covered include servers, workstations, desktop computers, laptop/ notebook/handheld computers, communications equipment, photocopiers, telephones, facsimile machines and audio visual equipment installed or operated on behalf of the Company at any location.

Objectives

The objectives of the IT policy and its supporting policies are to:

- Provide systems that are suited to their purpose;
- Provide and maintain safe IT equipment in a suitable environment, and to ensure safe working practice in the operation of IT equipment;
- Ensure that the Company achieves best value in its IT provision;
- Ensure that the Company's IT facilities are adequately secure;
- Ensure that users are aware of and fully comply with the relevant legislation, policies, procedures, guidelines and standards; and
- Ensure safe, socially and environmentally responsible disposal of equipment.

Responsibility for IT policies

It is the responsibility of each member of staff, to ensure their understanding of and compliance with this and associated policies.

Compliance with legislation

The Company has an obligation to abide by all relevant legislation. This policy and supporting policies, procedures, guidelines and standards must satisfy all applicable legislation. This obligation formally devolves to all users, who may be held personally liable for any breach of the legislation.

If anyone finds an inconsistency between policies and legislation, or between individual policies, they must bring this to the attention of the Chief Technology Officer (CTO).

Health & Safety

The Company will provide and maintain equipment that is safe in the context of its intended use. Individual users have a responsibility to operate these systems safely and report any defects.

All users must follow manufacturers' instructions or handbooks in the installation and operation of IT systems, and should consult the IT department when advice is needed.

Environmental Responsibility

All systems within the scope of this policy will be acquired, operated and disposed of in an environmentally responsible manner.

Intellectual Property Rights etc

No user may copy programs or information to paper, removable media (such as floppy disks), non-removable media (such as hard discs) or to portable computers except where explicitly allowed by the license agreement/contract and where no copyright or intellectual property right is infringed.

Theft and Misuse

Unauthorised removal of the Company, owned, leased, rented or loaned IT equipment, software or data from Company premises constitutes a theft.

No user may interfere with protection systems. This includes any device which is provided to prevent removal or theft of equipment, any software or configuration that detects or prevents virus infection and any software or configuration that prevents the running of non-approved software.

No user may install or use software or systems which are not licensed for use.

Company systems may not be used to transmit, store or access text, images, recordings, scripts, programs or telephone calls that contain:

- Material likely to contravene current legislation such as sexist, racist, homophobic, xenophobic, pornographic, paedophilic or discriminatory material, except in the legitimate pursuit of valid pre-authorised research;
- Text, images or recordings to which a third party hold copyright or other intellectual property right, without the written permission of the right holder;
- Material that is defamatory, libellous, slanderous or threatening;
- Material that could be used to breach computer security or to facilitate unauthorised entry into computer systems;
- Material that is likely to prejudice or seriously impede the course of justice in UK criminal or civil proceedings;
- Material containing personal data as defined by the Data Protection Act 1998 and The General Data Protection Regulation (GDPR) 2018 unless the subject's permission has been explicitly given in writing.

Accessibility

Where electronic information is provided with the intention of being generally accessible, this information should be in a suitable form for those with disabilities to gain access to the information wherever practicable.

The Company will, wherever possible, make suitable provision for legitimate users with disabilities to access company information using appropriate information technology.

Conditions of Use for IT Systems

Principles

Company IT assets must be safeguarded, and operated and administered in the best interests of the Company.

Access to equipment and information

It is not normally permitted for users to allow someone else to log in under their username in order to make use of their file space or for any other purpose. If temporary access needs to be given to someone else, the usual practice would be for the normal user to perform the login process. If, for legitimate operational or training reasons and with the approval of their line manager, a password is divulged to someone else, the password must be changed soonest.

A user must login to a shared system only under a username which he or she has been allocated. Logging in to a machine using someone else's username, password or PIN number is an offence unless it is for legitimate operational or training reasons and with the approval of their line manager. A manager may consider it necessary to access an absent member of staff's files or email messages in order to maintain continuity of service. Where the absent member of staff's password is not known, the IT Department should be contacted in order to gain access.

Security of passwords and PIN numbers

It is the responsibility of all users to maintain the security of their own passwords and PIN numbers. Any user who fails to take reasonable steps to do so breaches this policy and may be liable for any consequences which follow if another person makes use of one of them. It is good practice to periodically change your password, and if you suspect that your password has become known to someone else you should change it immediately. Passwords should be chosen with care: do not use a dictionary word or a name, and include a number and a symbol. Passwords should not be made readily accessible: treat passwords safely and securely.

Use and security of equipment and information

IT resources may only be used for the purpose they are intended and in the way these systems are configured. Only IT Department staff, approved contractors or others with approval from the IT Manager are permitted to change the use or system configuration IT equipment and software.

Users are permitted to change user preferences to suit their working practice or style provided the settings do not compromise security or alter operability for others.

No user may use a computer system in any way which puts files or information belonging to someone else at risk of damage. In particular, knowingly introducing a computer virus is a serious offence which may result in disciplinary action.
Users must cooperate with the IT Department in preventative or remedial action concerning equipment and data security.

Publishing or communicating without the authority of the CTO any information which allows someone else to breach the security of the computer systems is an offence. Examples are users' passwords or loopholes in system security which a user may come across accidentally whilst making legitimate use of the facilities. All users must inform the IT Department when they find evidence of failures or weaknesses in security. The Chief Technology Officer has the authority to give information which allows a breach of security, but this would normally be confined to testing and detection purposes only.

Systems may not be used to transmit, store or access text, images, recordings, scripts, programs or telephone calls that:

- Will consume sufficient network or server resource as to impede the effective use of systems by other users;
- Is likely to incur unwarranted costs on the Company;
- Is likely to involve users or support staff in wasted time;
- Contain misleadingly out-of-date information;
- Contain inaccurate or deceiving information;
- Seeks to unreasonably trivialise, insult or degrade other individuals, groups or bodies, or infringe others' human rights;
- Use techniques that capture or otherwise display third party information in such a way as to give the impression that they come from anywhere other than the original source.

No material may display the Company logo or name, or otherwise give the impression that they are official Company documents other than documents relating to business.

Monitoring

You are provided with the use of the computer system and telephone to assist in the performance of your job. You should have no expectation of privacy in any communications, or anything you create, store, send or receive using company Facilities. The Company has the right, and where appropriate intends to exercise such right, to monitor, access, intercept, record, retrieve or delete any matter stored, created, received or sent using the Facilities, whether personal or otherwise. This may include, but is not limited to, telephone conversations, internet sites, chat and newsgroups, file downloads/uploads, screenshot recording and all communications sent and received by users.

Monitoring of the Facilities

You must be aware that the Company's security system is capable of recording every document or file created, E-mail and file transfer, internet site accessed, use of chat room and newsgroups for every user. No employee should have an expectation of privacy in relation to electronic records or communications using the Company's systems.

The Company reserves the right to use covert surveillance in cases where any suspected dishonesty may have taken place either in relation to the activities of employee(s) or third parties or in cases where there may be a suspected breach of contract, e.g. breach of a restrictive covenant or breach of confidential information, such as would be likely to damage the business or reputation of the Company.

Social Networking and Video Sharing Websites

Any employee, who logs onto and uses social networking and video sharing websites or blogs, including personal use outside the workplace, must not:

- Publicly identify themselves as working for the Company, make reference to the Company or give any information from which others could ascertain the name of the Company
- Conduct themselves in any way that may cause a problem to the Company or bring the Company into disrepute
- Use their work email address when registering
- Allow the use of these sites or blogs to undermine the working relationships between employees and/or customers of the Company
- Refer to any personal information and make any derogatory remarks relating to any colleagues, customers, contractors or suppliers without their express consent, including when the individual is not expressly named by the Company believes they are identifiable
- Make any comments about colleagues that could constitute unlawful harassment, bullying or discrimination
- Disclose any Company trade secrets or confidential information relating to the Company, its employees, customers, suppliers or any information which could be used by any of the Company's competitors.

Any contravention of these rules, whether inside or outside the workplace, will subject the employee to serious disciplinary action which, depending on the seriousness of the offence, may amount to gross misconduct and could result in summary dismissal.

Downloading Information from the Internet and File Sharing

It is not permitted at any time to download material from the internet that is subject to copyright including music, film and business software.