Live Active Leisure

INFORMATION TECHNOLOGY POLICY

Introduction

Live Active Leisure [the Company] relies heavily on information technology and computer systems, and the security, confidentiality, and accuracy of the systems and information is of vital importance to the working of the Company.

The purpose of this policy is to ensure ***Our People*** understand the way in which technology should be used in the workplace. This written policy aims to inform ***Our People*** of their responsibilities and limits when accessing the Company's technology and to protect the Company against vicarious liability by inappropriate or illegal actions by ***Our People***. It also aims to educate system users about legal risks they may inadvertently take.

The Company recognises the requirement for personal use of Company computer equipment and software including accessing the internet for personal use, however the Company's objective is to ensure the personal use of equipment and software does not interfere with individual work responsibilities and that ***Our People*** understand that any personal use does not guarantee privacy of correspondence.

To maintain all the computer equipment, systems and information in a sensibly controlled environment and to ensure compliance with the law, there are a number of guidelines to be observed and legislation to be considered.

Legislative Background

The use of computers and computer systems and the associated security arrangements are covered by the following Acts of Parliament:

Data Protection Act 1988

The Data Protection Act 1998 is an Act to make new provision for the regulation and processing of information relating to living individuals (i.e. personal data), personal data and how that data is used. The Company's Data Protection Policy details the provisions of the Data Protection Act 1998. The Data Protection Principles set out in the Act operates as a mandatory code of conduct for obtaining, holding and processing personal data. They require the holder to use the data for only one or more specified and lawful purposes; they control disclosure to third parties and the length of time for which the data may be held; they require individuals to be informed of the fact the data is being held and to be given access to the information. Individuals may have inaccurate data corrected or erased and there are also security requirements to protect the data that is held.

Copyright, Deigns and Patents Act 1998

The Copyright Act specifically extends the principle of copyright to cover computer software and digital and electronic publications. Under this act downloading is prohibited without agreement from the copyright holder. Furthermore downloading an unlicensed copy, or using and unlicensed copy, of computer software is an offence.

Protection from Harassment Act 1997, Defamation Act 1996, Discrimination law (age, sex, race, disability, sexual orientation and religion and belief)

These laws all protect individuals from suffering abuse, harassment, defamation or discrimination at the hands of others. E-mail communications and the downloading of inappropriate images from the Internet may contain language or graphics that are insulting, demeaning or unlawful.

Whilst the perpetrator of the message or download may be legally liable for damage caused, the Company may also have vicarious liability for the actions of their employees.

Human Rights Act 1998

Employees have reasonable expectation of privacy in the workplace, employers are recommended to provide workers with some means of making personal communications which are not subject to monitoring. The Company will attempt to preserve the privacy of personal communications and will not access the contents of any communication without reasonable cause and will advise staff, if possible, when this is to happen.

Contract Law

It is just as possible to make a legally binding contract via email as it is by letter or orally. Employees need to be aware of the danger of inadvertently making contacts on behalf of the Company.

Computer Misuse Act 1990

The Computer Misuse Act states that both unauthorised access to a computer or computer system and the misuse of a computer or computer systems are offences and is generally concerned with the problems of 'hacking' into computer systems.

Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988

These Acts are concerned with material that might be criminal, cause harm to young persons or be otherwise unlawful. In the workplace downloading certain images from the Internet might subject an employee to be charged with criminal behaviour.

Computer Equipment

- Facility Operations Managers are responsible for all computer equipment under their control and for its proper use. Individual users are responsible for the proper use and treatment of computer equipment to which they directly have access
- The use for equipment for purposes not directly concerned with the business is allowed only with the permission of the Facility Operations Managers
- Only Company staff authorised by the Facility Operations Managers may operate computer equipment. Authorisation is considered granted when the login facilities are issued
- Computer equipment must have security facilities appropriate to the sensitivity of data held. The Health & Safety & Estates Manager will offer advice on what is considered appropriate security
- Facility Operations Managers are responsible for the physical security of locations within their facility where computers are used

Computer Systems and Data

- Software licenses are not transferable and as such all computer programs and data developed for, or acquired by, the Company are for sole use of the Company
- New computer programmes may only be used on Company computer equipment with the approval of the Health & Safety & Estates Manager
- The storage or use of computer games or other leisure software on Company computer equipment, is only allowed with prior authorisation from the Health & Safety & Estates Manager and will only be considered if educationally beneficial
- The Health & Safety & Estates Manager, supported by the HR & Administration Officer is responsible for the notification of personal data held and processed on computer equipment
- Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is prohibited

- Unauthorised disclosure of information from computer input or output is prohibited

- Waste computer output must be disposed with due regard to its sensitivity. Individual facilities will be responsible for ensuring that confidential printed output is disposed of correctly. Advice on secure disposal can be sought from the Health & Safety & Estates Manager

Security Systems

- Terminals or personal computers must not be left unattended when signed on

- Passwords must not be disclosed to any other persons unless in an emergency situation

- The use of another person's password is prohibited, unless in an emergency situation and with the consent of the password holder

- Passwords, which have been forgotten or locked, will be reset by the Information Systems & Technology team at Perth & Kinross Council when adequate proof of identity and authority is given

- Breaches of security must be reported to the Health & Safety & Estates Manager and appropriate Facility Operations Managers

- Any computer connected to any Company network must have appropriate anti-virus facilities. The Information Systems & Technology department within Perth & Kinross Council is responsible for the installation and maintenance of this software

Internet Security

The Company provides access to the Internet as a business tool. In general, Internet access should only be used for Company related business purposes, (ie to communicate with customers and suppliers, to research relevant topics and to obtain useful business information). Unnecessary or unauthorised Internet usage causes network and server congestion with unlawful Internet usage potentially attracting negative publicity to the Company, as well as exposing the individual and the Company to legal liabilities.

All existing Company policies, especially (but not exclusively) those dealing with copyright, software licensing, confidentiality, Data Protection and information security, misuse of Company resources and harassment, apply to anyone using Company provided Internet access.

- The Company has in place, through Perth & Kinross Council, security software to record and monitor all web sites, all email, newsgroup and chat messages and all file transfers in and out of the Company network. All Internet activity will be monitored and access limited to those who demonstrate a genuine business need. Passwords must be kept confidential

- Any, and all files stored on the network or in private areas may be inspected to ensure that they comply with Company policy

- To ensure full disclosure of Company documents, the use of private areas and desktops are in the main prohibited. Company documents must be saved on the Company network to allow full access by other users. Usage of your desktop for anything other than shortcuts must be approved by the Health & Safety & Estates Manager

- The display of any kind of sexually explicit image or document on any Company system is in contravention of the Company's harassment policy. Sexually explicit material may not be archived, stored, distributed, edited or recorded using the Company's network or computing resources

- The Company uses independently supplied software and data to identify inappropriate or sexually explicit sites and access to such sites may be blocked. Any cases of Company networks or computers being used to access sexually or indecent material relating to subjects who are, or appear to be under 16 will be reported to the police immediately

- Any software of files downloaded from the Internet via Company provided access become the property of the Company. Software licensing rules must be observed. Software may not be uploaded without formal authorisation from the Health & Safety & Estates Manager

- Images, audio and/or video constitute significant data traffic and may not be downloaded unless there is an explicit business-related use for the material

- The Company's Internet facilities may not be used to download entertainment software or games, or to play games individually or against opponents over the Internet

- The Company's Internet facilities may not be used knowingly to disable or overload any computer system or network or to circumvent any system intended to protect the privacy or security of another user

- Users of the Company Internet facilities must identify themselves honestly and accurately when communicating with other users

- Only those authorised to do so may issue statements, news releases or information on behalf of the Company. Company provided computers, networks, and Internet access may not be used for electioneering and related political purposes

- Blogging on social networking sites during working time is classed as unacceptable usage of the Company's equipment and systems. Discussing the Company on such social networking sites, either during working hours or out with, that causes harassment to another employee or defamatory statements about the Company will be dealt with under the Company's disciplinary and grievance procedures. Furthermore confidential matters should not be discussed in such forums. For more details regarding employees use on Social Media please refer to the Company's Social Media Policy

Email Security

- All email messages form part of the Company records. The Company reserves the right to access and disclose as necessary all messages sent over its email system, without regard to content. This may be to find lost messages, to comply with investigations of wrongful acts or to recover from system failure. Under the Freedom of Information (FOI) and related Acts the Company is obliged to make available all e-mails deamed by the Company or the Information Commisioners Office as relevant to an FOI request.

- Since personal messages can be accessed by the Company without prior notice, email should not be used to transmit any messages you would not want read by a third party. Employees should not assume email messages are confidential

- Personal use of email by employees is allowable but should not interfere with or conflict with business use. Personal messages will be treated the same as other messages but must be labelled as personal email in the Subject box. Employees should exercise good judgement of the personal use of email, ensuring that it does not interfere with their daily work requirements

- Access to another employee's email account or mailbox is acceptable provided that permission has been granted by the account holder through the delegates option in Outlook. During periods of long term absence Line Managers may request access to an employee's e-mail account by contacting the Health & Safety and Estates Manager.

- A standard disclaimer will be inserted on all outgoing external email. Signature file or message text must disclose limitations of an employee's authority. The correct signature file can be obtained from the HR & Administration Section at Company Head Office

- All misaddressed email, whether internal or external, must be returned to the sender notifying him or her that the address is incorrect. Confidential or personal email should not be forwarded to other individuals, mailing lists, or newsgroup without the original sender's express or implied consent

- Email must not be misused – examples of misuse include:

  a) Transmissions which include sexually-explicit messages, inappropriate cartoons or jokes; unwelcome propositions or love letter; ethnic or racial slurs; or any other message that can be construed to be harassment or disparagement of others based on their gender, race, sexual orientation, age, disability, marital status, religion, national origin, or political beliefs

  b) Broadcasting unsolicited personal views on social, political, religious or other non-business related matters

- Anyone receiving threatening, intimidating or harassing email should report the matter to his or her Line Manager. If annoying or unsolicited email from the same sender or address persists, Information Systems & Technology at Perth & Kinross Council should be informed when appropriate technical measures may be implemented

- Any contravention of the above provisions may result in disciplinary action being taken against an individual

Email Etiquette

The electronic mail system is a means of communication which:

- Identifies the originator of the message
- Identifies the destination(s) of the message
- Records the date and time the message was sent
- Records the date and time the message was received
- Records the date and time the message was opened
- Records the date and time the message was deleted
- Allows the message to be printed
- Allows the message to be saved on disk
- Allows the message to be forwarded to another mailbox user
- Allows the message to be replied to
- Can notify that a message has been received
- Can notify that their message has been received
- Can notify that their message has been opened

When to Use

- Arrange meetings
- Convey brief information
- Confirm arrangements
- Provide consistent message to a group(s)
- One-to-One conversation
- To leave messages (when person unavailable)
- Append documents as attachments for printing by the recipient

When Not to Use

- Message is sensitive (staff, financial, security, etc)
- Message is complex
- Message is lengthy
- Message is formal communication
- When conversation is more appropriate
- Advertising

- Electronic mail is traditionally informal means of communication and therefore can be considered equivalent to a verbal conversation. However, unlike verbal communication, electronic mail is always recorded and can be printed. It is therefore vital that personal messaging be restricted

- The tone of a message should also be carefully considered given that, while a phrase may be acceptable with verbal intonation, on the printed page a message may seem irrelevant, silly or even derisory if it is not read in the same spirit that it was sent

- Check your mail regularly, at least once a day

- Ensure a meaningful subject heading is used, however you should avoid at all times the use of personal details in the subject heading, for example an employees name or customers name

- Lay out your message clearly – use of block capitals should be restricted – this can be interpreted as SHOUTING. Keep the message succinct, longer documents should be sent as an attachment to you message (ensure that the recipient can read your word processing format)

- Distinguish between whom the mail message is to and who gets copies. (The recipient may require to take action on the message, copies are for information only)

- No junk mail. Personal one-to-one messaging is OK, but not within groups

- No images that would be deemed offensive, pornographic or inappropriate to your audience

- Although you can e-mail to anyone in the organisation, whatever level, you should judge your audience and the tone of your message carefully

- Always reply to an email promptly, where a response is required and at least within three working days

- Remember that there is no guaranteed response time with electronic mail. You may not be aware that annual leave or sickness is preventing a reply being sent. If the message is important enough to require a response within a defined time, the onus is on you to ensure the correct type of communication is used

- When you are on annual leave or out of the office for an extended period of time ensure that you use the out of office assistant detailing when you are due to return and a contact phone number of an appropriate person within your office who can assist or pass on the request for action in your absence

- There is a resource implication of using electronic mail. Mail messages, which are sent to and received in your mailbox, require disk space on your file server and, as such cannot be allowed to accumulate without a limit being reached. It is therefore necessary that you delete mail messages both from your In and Out Boxes regularly. If you require to keep any messages, create folders to store them

- Email should never be used as an alternative for talking

Inappropriate Use of Computer Equipment, Data, Email & Internet

The Company relies heavily on information technology and computer systems, and the security, confidentiality, and accuracy of the systems and information is a vital importance to the working of the Company

Therefore failure to adhere to the policy or abuse of the above provisions may result in disciplinary action being taken against the individual(s) involved.

Any breach of the above or suspected breach will be investigated in accordance with the Company's Disciplinary procedure.