IT Acceptable Use Policy

Internet Usage, Email usage, Use of ICT Equipment, Information Security & Data Handling

Contents

Revision History

Issue	Date	Comments
1.0	08 04 2009	Renamed as IT Acceptable Use Policy, previously version 1.5 of the ICT Policies Manual.

1. IT AND COMMUNICATIONS TECHNOLOGY POLICIES

1.1 Introduction

IT and Communications Technology (ICT) is an essential resource for South Lanarkshire Leisure and the Trust has invested considerable resources to provide an effective and up to date network of services. To continue to operate effectively however the technology relies on users observing relevant policies and procedures.

This document defines a set of acceptable usage policies that are to be applied when using the South Lanarkshire Leisure ICT facility. This section provides an overview of these policies.

1.2 Basic principles

As with all Trust equipment and facilities the ICT network and associated equipment is provided primarily to further the Trust's interests and objectives. Whenever ICT equipment is being used for business use the relevant procedures and instructions should be adhered to.

In addition however some of these facilities can also be used by authorised users for their personal use.

This personal use:

- Should not interfere with the performance of official duties.
- Should not take priority over work responsibilities.
- Must not distract other employees from their work.
- Should not incur unwarranted expense on South Lanarkshire Leisure.
- Should not have a negative impact on South Lanarkshire Leisure in any way.
- Should follow relevant codes of practice.
- Should be lawful.
- Must comply with relevant South Lanarkshire Leisure's polices and procedures.

Any breaches of this policy will be viewed very seriously. They may be regarded as gross misconduct and may result in action being taken under the Trust's disciplinary procedures.

Specific codes of practice and guidance documents are available and provide more information on how to best use the internet and intranet as well as how monitoring is carried out, these are available on the intranet or from the HR section.

1.3 Internet and intranet use

Users of the Trust's ICT network can access the internet and intranet but this is monitored and reported. Each visit made to any website is traceable to the South Lanarkshire Leisure account that accessed that site, therefore any activity engaged in while on a website may affect South Lanarkshire Leisure.

The Trust has in place filtering and blocking software that regulates the sites that can be visited but users still have a responsibility to observe the basic principles listed in section 1.2.

Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights. You must make sure that all appropriate copyright and intellectual property rights as well as licensing requirements are observed. The ownership and licensing of information and software are of particular concern due to the penalties that can arise from breaching their terms of use.

1.4 Email use

Personal use of email is not prohibited provided this is carried out in the employees own time and observes relevant codes of practice and guidance documents. This use must also recognise and adhere to all relevant South Lanarkshire Leisure policies for example the Dignity at Work policy.

Users of the Trust's email system should not have any expectation of privacy when they use this facility and there are occasions when email content will be examined. These include the following:

- Accessing emails to provide evidence that a business transaction took place.
- Making sure South Lanarkshire Leisure's business and security procedures are adhered to.
- Training and monitoring standards of service.
- Preventing or detecting unauthorised use of South Lanarkshire Leisure's communications systems or criminal activities.
- Maintaining the effective operation of South Lanarkshire Leisure's ICT network.

1.5 Use of ICT equipment

The Trust will issue ICT users with equipment to enable access to the ICT network. This includes the keyboard, mouse, screen, disk drives, printers, memory and mobile devices like Personal Digital Assistants (PDA's) or Blackberries.

Information Technology Services are responsible for buying, leasing, installing and locating this equipment and each employee has a personal responsibility to look after and protect Trust assets.

If you need to use a computer or change the use of your present one, please contact our IT Business Officer to discuss your service needs.

Any required moves of equipment must be raised as a request for service through our IT Business Officer.

Only connect devices to the USB ports on your computer if you have the explicit authorisation of your line manager and you know the device to be virus free. Never connect devices that have not been approved by IT Services.

With the exception of portables, (laptop computers, PDA's and Blackberries) computer equipment must not be moved or disconnected.

Trust issued ICT equipment must not be removed or modified in any way.

1.6 ICT software

Software installed on the Trust's ICT equipment is provided to enable business applications to run.

A standard set of end user computer software products is available, chosen to provide a balanced and up-to-date coverage of most business needs. It is continually reviewed to keep in step with advances in technology.

You should consult with our IT Business Officer to evaluate your end user computing software needs. They may already have information on additional or alternative products and can achieve a competitive price. If a business application is needed, again you should contact our IT Business Officer to discuss your needs. Information Technology Services will ensure that all technical considerations relating to your desktop or laptop computer are addressed.

Any Software used on Trust IT equipment must be authorised and acquired legally. This is an individual and department responsibility. Information Technology Services will hold and maintain licenses for standard desktop systems and application software.

To be legal, the software must be registered for Trust use by Information Technology Services. Licensing agreements require that software is used only on the equipment for which it is authorised. This is controlled by means of an inventory.

There is a technical guideline on Legal & Ethical use of software. You can get a copy of this guide from our IT Business Officer.

To be authorised, the business use and purchase cost of software must be approved by your own line manager in consultation with our IT Business Officer.

Do not install, move, or copy software, change any system files or duplicate copyright document images. Software must only be installed or downloaded by, or with the agreement of, the authorised Information Technology Business Officer.

Do not install and/or hold games or ANY other non-business related files or programs on Trust computers. NEVER load or install images onto Trust computers that may offend or contravene any of the Trust's policies or procedures.

Only use authorised screen savers on your PC. All authorised screen savers are supplied at time of PC installation. Screen savers downloaded from the internet are NOT authorised.

1.7 Information security – user responsibilities

Information and the Information and Communications Technology systems and networks which deliver it are critical business assets. Their security is essential to the Trust's effective operation. This means we must make sure that information can be accessed only by appropriately authorised people and that it will be accurate and available whenever they need to use it.

South Lanarkshire Leisure is committed to doing this and will take steps to:

- protect our information and IT assets – hardware, software, infrastructure and data – against security threats
- enforce an effective Trust-wide Information Security Policy
- help users understand the importance of securing these assets as part of our everyday work, and
- make sure we follow relevant laws.

South Lanarkshire Leisure employees, as well as any working partners, will be provided with appropriate access to the equipment and systems they need to do their work effectively. Everyone using these has a direct responsibility for the security of the information assets.

Access to these information assets and IT systems will be controlled using specific accounts that must be used by the authorised user only. Authorised users will be responsible for actions recorded against that account.

Information security is everyone's responsibility. As a user you must understand and follow this policy. You must also immediately bring to the attention of your line manager or IT Help Desk (01698 455656) any instances of suspected or actual misuse which may compromise this Policy.

As a responsible organisation, South Lanarkshire Leisure will take steps to ensure that this policy is being adhered to. Everyone who uses South Lanarkshire Leisure information systems, which includes telephones, software, hardware, infrastructure and data must understand this Information Security Policy, and any other associated guidelines, and fully comply with them.

The Executive Directors of South Lanarkshire Leisure have agreed and issued an information security policy that recognises the importance and value of information to the Trust as well as the need for compliance with this policy document.

This important policy affects the use of ICT equipment and places responsibilities on the users.

Information Management – User Responsibilities

South Lanarkshire Leisure deals with a wide variety of information and needs to do this effectively to deliver services to its customers and partners. If you use this information, or the Information and Communications Technology systems and networks, you have an essential part to play and must follow the regulations that apply. This document summarises the responsibilities placed on you and identifies relevant Trust policies and codes of practice. Copies of these are available as detailed in the table below – you should make yourself aware of these and understand how they affect you.

Note that, in many cases, there is a legal obligation on the Trust to both enforce and monitor the implementation of these responsibilities and therefore any breach would be viewed as serious, especially where it is a breach of the Trust's Code of Conduct

As a user you must:

- Understand the nature and sensitivity of any information you deal with.
- Ensure information is retained securely, your line manager, HR Manager or the IT Help Desk (01698 455656) will provide further guidance about this.
- Use any IT equipment sensibly and observe the relevant codes of practice and guidance documents that apply.
- Ensure that any requests made of you for information are dealt with in accordance with the relevant procedures.
- Report either to your line manager, your HR Manager or the IT Help Desk any problems or issues you experience when using either the IT facilities or observing these responsibilities.

Information Security – Good Practice

- Data files should only be copied for authorised and official purposes.
- Attempting to gain access to information for any purpose other than that related to your work duties is strictly forbidden and unlawful.
- Unauthorised use of a password or user-id to access a computer system is prohibited.
- ICT equipment that is not owned or leased by the Trust must not be connected to the South Lanarkshire Leisure network.
- Passwords are not to be divulged to colleagues and must be kept private.
- ICT equipment that is logged on to the network must not be left unlocked when unattended.
- Do not leave ICT equipment unattended and visible in your car.

If reckless action or deliberate neglect by an employee leads to a breach of security or code of practice, appropriate action will be considered in accordance with the Trust's disciplinary procedures.

2. USE OF TRUST ISSUE ICT EQUIPMENT

2.1 General Principles

The Trust is heavily dependent on computer systems and information to achieve its aims and objectives, and recognises the importance of keeping data, information and equipment secure. The Trust is also committed to complying with the laws governing the use of information and the use of computer equipment. The Trust and its employees at all levels are legally required to follow good security and business practices by complying with the appropriate legislation.

This legislation places a number of obligations not only on the Trust but also on users of the Trust's ICT network and computing facilities. The legislation, while extensive, is there to protect the Trust and its employees. If you have any queries or concerns relating to these please contact your line manager or the IT Helpdesk. If reckless action or deliberate neglect by a member of staff leads to a breach of security or code of practice, appropriate action will be considered in accordance with the Trust's disciplinary procedures.

Your line manager will authorise you to use computer systems. Do not attempt to use equipment, software or data unless you are authorised to do so.

✔ You should report any observed or suspected breach of this code, or of security to your line manager.

This includes information processed on Trust computer systems.

✔ Follow this code of practice. If in doubt, contact your IT Business Officer.

Hardware

Hardware is the physical equipment used in a computer system. It includes things like the keyboard, mouse, screen, disk drives, printers, memory and mobile devices like Personal Digital Assistants (PDA's) or Blackberries.

Information Technology Services are responsible for buying, leasing, installing and locating computer equipment. Through centralisation, equipment is purchased or leased at competitive prices and compatibility is maintained. If you need to use a computer or change the use of your present one, please contact our IT Business Officer to discuss your service needs.

Any required moves of equipment must be raised as a request for service through your IT Business Officer.

Only use the USB ports on your computer if you have been authorised to do so by your manager. Only connect devices that have been authorised by IT Services and you know to be virus free.

With the exception of portables, (laptop computers, PDA's and Blackberries) you must not disconnect or move any computer equipment. Call-outs to fix any equipment after an unauthorised move will be subject to an extra charge to the department's cost centre.

You must not remove, insert or modify any computer components (including boards and cards).

Software

Software is provided to enable business applications to be run. A standard set of end user computer software products is available, chosen to provide a balanced and up-to-date coverage of most business needs. It is continually reviewed to keep in step with advances in technology. You should consult with our IT Business Officer to evaluate your end user computing software needs. They may already have information on products and can achieve a competitive price.

If a business application is needed, again you should contact our IT Business Officer to discuss your needs. Information Technology Services will ensure that all technical considerations relating to your computer are addressed.

Any Software used on Trust IT equipment must be authorised and acquired legally. This is an individual and department responsibility. Information Technology Services will hold and maintain licenses for standard desktop systems and application software.

- To be legal, the software must be registered for Trust use by Information Technology Services. Licensing agreements require that software is used only on the equipment for which it is authorised. This is controlled by means of an inventory.
- There is a technical guideline on Legal & Ethical use of software. You can get a copy of this guide from your IT Business Officer.
- To be authorised, the business use and purchase cost of software must be approved by your own line manager in consultation with Information Technology Services
- Do not install, move, or copy software, change any system files or duplicate copyright document images. Software must only be installed or downloaded by, or with the agreement of, authorised Information Technology Services staff.
- Do not install and/or hold games or ANY other non-business related files or programs on Trust computers.

NEVER load or install images onto Trust computers that may offend or contravene any of the Trust's policies, for example, Dignity at Work or Equal Opportunities.

Only use authorised screen savers on your PC. All authorised screen savers are supplied at time of PC installation. Screensavers downloaded from the internet are NOT authorised.

You can arrange access to computer systems by contacting our IT Business Officer. They will organise this by contacting the relevant people within Information Technology Services.

You should only copy data files for authorised and official purposes.

Do not attempt to gain access to information for any purpose other than that related to your work duties. Unauthorised use of a password to access a computer system is strictly forbidden and unlawful.

If you have your own computer or personal organiser, they must never be connected to the South Lanarkshire Leisure network.

Never ask to use a colleague's password or user-id. Get authorisation from your line manager for your own password. If you have forgotten your own password, ask your system administrator to issue a new one.

Do not use a password belonging to someone else and keep your own password private.

NEVER leave your PC logged on and unlocked when unattended.

Do not leave computer equipment unattended and visible in your car.

Lock your PC if you are going to leave it unattended and log out if you will be away for a long period of time.

External Networks such as the Internet, allow mail and data to move between computer systems, potentially world-wide, but the significant security risks mean rigorous control is needed.

It is essential to discuss your business needs for any external communication links with our IT Business Officer, who will talk to the relevant people within Information Technology Services who in turn will evaluate the risk and if appropriate, process the request.

Passwords

Change your password at regular intervals, every month. Passwords should be at least 6 characters long. Choose your password with care taken to avoid easily guessable ones.

You should protect sensitive data in databases, spreadsheets and word processing documents from unauthorised access by using the separate password protection facilities included in the software.

Malware

Malware such as virus programs are malicious and aimed at damaging or destroying data held on computers, or more dangerously, held on the network. Viruses are also used to simply disrupt normal business operations or disclose information held on those computers. Malware infections could potentially cost the Trust, thousands of pounds.

NEVER allow any disk or storage device to be used in a PC or laptop unless you are confident it is free of malware. Anti-Virus software and other relevant security updates will be installed on your PC, and will be updated in line with security needs.

You MUST NOT under any circumstances attempt to remove, stop or re-configure any part of the anti-virus or security updates installed on your PC.

Unless you have been specifically authorised NEVER use a Trust laptop to access a website other than via the corporate network.

If you suspect a malware infection, contact the Help Centre (01698 45 5656) immediately and they will investigate. Quick action is vital to prevent the spread of the virus or malware. Do not use your computer until it is checked out, using your computer may spread the infection.

Backups

Data which needs to be shared within your own department or with other departments, should be stored centrally. For users this would generally be on a network server or another central device. For those not attached to a server, important data should be held on the computer hard disk.

Back up all your hard disk data regularly. Managers and supervisors should ensure backups of hard disks are stored securely and adequate recovery procedures are in place for all essential data. If you are unsure what to do, contact our IT Business Officer.

Disposal of media and equipment

Computer equipment can be disposed of securely and safely by contacting our IT Business Officer. Computer equipment which is reusable can also be made available for recycling. Do not dispose of equipment yourself. Contact our IT Business Officer, and they will arrange to have this costed and done for you.

Health and Safety

You must use all computer equipment in accordance with Corporate and departmental health and safety guidelines. Guidelines on the use of display screen equipment are available from our Health and Safety Officer.

3. USE OF THE INTERNET AND INTRANET

3.1 Basic principles

This guidance applies to you if you are a user of South Lanarkshire Leisure's Intranet or Internet facility. Any inappropriate use of South Lanarkshire Leisure's communications systems may lead to action as defined under South Lanarkshire Leisure's disciplinary procedures.

It is important that you read this code of practice carefully. If there is anything that you do not understand, please discuss it with your line Manager or IT Business Officer.

The main advantage of the internet and intranet is that they are an extremely easy and informal way of accessing and disseminating information. However, the same principles apply to information exchanged in this way as apply to other means of communication. Bear in mind at all times that when visiting an internet site the unique address for your computer (your IP address) can be logged by the site you visit, so your South Lanarkshire Leisure email account can be identified. This means that any activity you engage in is attributable to South Lanarkshire Leisure and directly traceable to you.

Do not use the internet and electronic mail therefore, for purposes which would be subject to disciplinary or legal action in any other context. If you are in doubt about a course of action, take advice from your line manager or the IT Business Officer.

Intranet and internet access are intended to be used for business purposes, and we do expect you to use them responsibly, in line with the all relevant South Lanarkshire Leisure policies and codes of practice.

Personal use of the intranet and the internet is not prohibited provided this is carried out in the employees own time and observes relevant Trust policies, procedures and codes of practice.

Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights. You must make sure that all appropriate copyright and intellectual property rights as well as licensing requirements are observed. The ownership and licensing of information and software are of particular concern due to the penalties that can arise from breaching their terms of use.

3.2 Internet filtering, monitoring and recording

Computers attached to the South Lanarkshire Leisure network access the internet do so in a controlled manner that verifies that the sites visited are valid suitable for access by Trust equipment. To do this the Trust pay for and make use of proprietary blocking tools that categorise every location on the internet. Unsuitable sites are blocked and cannot be accessed.

These tools record every time a computer attached to the South Lanarkshire Leisure network accesses the intranet or internet and maintain a log of each site visited, the time spent on that site and each blocked request. This log is routinely analysed and submitted on a regular basis to SLL for review and instances of inappropriate use are referred to SLL for action.

Further, detailed reports, listing the total Internet Usage by employees, including the top sites visited, are distributed to line managers who asses that Internet Usage is appropriate to the business and compliant with Trust Policies.

These logs are retained for 6 months as per the requirements of the Data Protection Act, you are entitled to inspect these. Should you require to do this, you can do this by asking your line manager or by contacting the Trust's IT Business Officer.

If an individual computer is the subject of repeated problems an investigation of content and usage history may be carried out either by IT Services or South Lanarkshire Council's Internal Audit. For example if a specific computer is repeatedly infected by computer virus programs a review of the websites accessed by that machine may have to be carried out.

3.3 Use of internet and intranet - guidelines

You should **NOT**

- Download any images, text or material which is copyright protected.
- Use unlicensed computer software.
- Use unauthorised computer software.
- Download any images, text or material which is obscene, likely to cause offence or infringe any of the Trust's policies, for example Dignity at Work or Equal Opportunities;
- Introduce software which is used to intercept data on a network or password detecting software
- Seek to gain access to restricted areas of the network
- Knowingly seek to access data which you know or ought to know to be confidential, unless authorised to do so.
- Introduce any form of computer viruses;
- Carry out other hacking activities.
- For your information, the following activities are criminal offences under the Computer Misuse Act 1990:
  - unauthorised access to computer material i.e. hacking;
  - unauthorised modification of computer material; and
  - unauthorised access with intent to commit/facilitate the commission of further offences.

You **SHOULD**

- When entering an internet site, always read and comply with the terms and conditions governing its use;
- If you have a need to download any software for business purposes, consult first with our IT Business Officer.
- Ensure that any software downloaded for approved business purposes only is properly licensed for use. (Licensed by South Lanarkshire Council).
- Follow all relevant Trust policies and codes of practice.

3.4 Personal use of the internet

Any personal use of the internet must firstly comply with the South Lanarkshire Leisure Code of Conduct for Employees. The following principles must also be followed. Personal use must:

- Not interfere with the performance of your duties
- Not take priority over your work responsibilities
- Not incur unwarranted expense on South Lanarkshire Leisure
- Not have a negative impact on South Lanarkshire Leisure in any way
- Follow the IT Acceptable Use Policy
- Be lawful.
- Comply with the South Lanarkshire Leisure Dignity at Work policy as well as all other relevant policies.

4. USE OF EMAIL

4.1 General Principles

How you communicate with people not only reflects on you as an individual but on South Lanarkshire Leisure as an organisation, and may have legal implications on you and on the Trust. Therefore, although we will respect your personal autonomy and privacy, we have established this code of practice to advise you what we expect from you and what you can expect from us in your use of email.

We expect you to use the Trust's email systems and facilities sensibly, professionally, lawfully, consistently with your duties, with respect for your colleagues and in accordance with South Lanarkshire Leisure's policies and procedures, for example the Code of Conduct and Equal Opportunities.

This code applies to you if you are a user of South Lanarkshire Leisure email facility. Any inappropriate use of South Lanarkshire Leisure's email systems may lead to action as defined under South Lanarkshire Leisure's disciplinary procedures.

It is important that you read this policy document carefully. If there is anything that you do not understand, please discuss it with your line Manager or IT Business Officer.

You must treat all of the information South Lanarkshire Leisure holds with great care. See the section on Information Security Policy – User Responsibilities for more information.

Particular care must be taken when using email as a means of communication as all expressions of fact, intention and opinion via email may be produced in court in the same way as any other Trust document. We therefore expect you to use email sensibly. Every mails sent externally will have the standard South Lanarkshire Leisure email disclaimer automatically attached.

Email is an extremely easy method of accessing and disseminating information. However, the same principles must apply to information exchanged in this way as apply to other means of communication used by the Trust.

Do not use email therefore, for purposes which would be subject to disciplinary or legal action in any other context. If you are in doubt about a course of action, take advice from your line manager.

As an employee, you should exercise due care when using email to collect, process or disclose any personal data and only process personal data on behalf of South Lanarkshire Leisure where it is necessary for your duties.

Email is intended to be used for business purposes, and we do expect you to use this responsibly, in line with the South Lanarkshire Leisure Code of Conduct for employees and with the IT Acceptable Use Policy.

Personal use of email is not prohibited provided this is carried out in the employees own time and observes relevant codes of practice, policies and procedures detailed above.

4.2 Email use – summary guidelines

Although e-mail is a very easy way to communicate and distribute information it is **not** secure. Before sending information by email first consider how sensitive that information is and assess the risks of it either being intercepted, sent to an incorrect email address or opened in a open office environment.

You MUST NOT

- Use a false identity in emails you send out
- Exploit mail servers or other systems to facilitate the widespread distribution of unsolicited and unwanted email
- Send confidential or sensitive information outside the Trust network unless you know you are sending it to a secure network or email address, if in doubt contact your line manager or the IT Business Officer.
- Allow third parties to read personal information in emails or attachments by leaving your screen in view of such third parties.
- Create or forward advertisements or unsolicited emails.
- Use the email facility to forward chain letters, or any other form of non business related mail, you are asked to forward on to a number of recipients.
- Read other peoples' emails sent to someone else without their express permission.
- Pass your password to any third party.
- Open electronic attachments if you are unsure of their source.
- Rely on the email system or any automatic archiving to store important business communications, contact the Records Management Service for advice on maintaining business records.

And you **SHOULD**

- Be cautious about putting any personal information in an email, see section 4.6 Sending Personal Data by Email.
- Note that the recipients of your emails, the originators of emails you receive and the content of all emails sent or received MAY be subject to scrutiny.
- Re-read email before sending them, as email cannot be retrieved once they have been sent.
- Virus check all attachments before saving them on your PC
- Follow the relevant policies and codes of practice.
- Store important email records in the email message format on a network drive, for more information contact the IT Business Officer for advice on maintaining business records.

4.3 Personal use of email

Any personal use of the Trust's email facility provided to you must comply with the South Lanarkshire Leisure Code of Conduct for Employees. The following principles must also be followed. Personal use must:

- Not interfere with the performance of your duties
- Not take priority over your work responsibilities
- Not incur unwarranted expense on South Lanarkshire Leisure
- Not have a negative impact on South Lanarkshire Leisure in any way
- Follow the IT Acceptable Use Policy
- Be lawful.
- Comply with all other relevant South Lanarkshire Leisure policies and procedures.

Multimedia and audio files

Due to the increasing amount of space taken up by multimedia files, such as photographs music and video, unless it is for legitimate business purposes it is forbidden to use the Trust's network or email system to send or broadcast multimedia or audio files. This includes photographs, audio, video files and Microsoft Powerpoint shows.

4.4 Remote access to the Trust's email system

This section describes the controls that are to be exercised by individuals who are granted the facility to access their Trust email account while not logged on to the South Lanarkshire Leisure ICT network.

It covers the various means of accessing email accounts that may be introduced by the Trust including Outlook Web Access, Blackberry®, mobile telephones, Personal Digital Assistants such as IPAQ, Psion Organisers, and similar data transmission devices.

Employees who are given this means of access must ensure that they are aware of, and comply with, these requirements and should sign and return any Conditions of Use section that apply.

Allocation of remote access privileges

Individuals who need to remotely access their email account should request authorisation from their line manager. The authorising line manager should contact the IT Business Officer.

Access will only be given after the user has recorded their acceptance of the conditions and responsibilities defined in this document.

No responsibility will be accepted by the Trust for any damage or performance deterioration in equipment not supplied by the Trust to access the Trust's email system.

Security of email and attachments

Not only is the Trust's email system one of its main tools for transmitting information but also email threads can often record how decisions are made and record information.

This information could often be classified either as confidential, restricted or personal information and must be dealt with securely. Whenever you remotely access your email account make yourself aware of the nature of the emails you expect to receive and consider if it is appropriate to open them outside your work environment.

This decision must be made by the remote user and take into account the location and equipment to be used. Factors that must be considered include:

- Is the computer used by anyone else?
- Can anyone else overlook the screen?
- Does the computer have up to date and adequate protection against virus and malware?

Should confidential or restricted information be made public this would breach the Trust's Information Security Policy and potentially cause serious repercussions for the Trust.

For this reason each user who remotely accesses their Trust email account must observe the good practices identified in this document and continue to follow the Trust's acceptable usage policy for email.

Particular care is required when opening or downloading email attachments:

- Do not open attachments unless it is essential to do so
- Do not leave copies of attachments on the hard drives computers that are not Trust equipment

Do not use remote access to the Trust's email system to send attachments unless you are certain the attachments are virus free. If possible ensure that the computer you use to access your email account has suitable virus protection in place.

4.5 Monitoring email use

South Lanarkshire Leisure has a duty to ensure that users of its email systems adhere to the necessary Trust policies and to this end will routinely monitor and report on employee usage.

This monitoring takes into account updated legislation and ensures a minimum level of personal privacy for employees in their employment.

South Lanarkshire Leisure will respect your privacy and autonomy in your electronic communications. However, in certain circumstances it may sometimes be necessary to access and record your electronic communications for South Lanarkshire Leisure's business purposes which include the following:

- Providing evidence of business transactions.
- Making sure South Lanarkshire Leisure's business and security procedures are adhered to.
- Training and monitoring standards of service.
- Preventing or detecting unauthorised use of South Lanarkshire Leisure's communications systems or criminal activities.
- Maintaining the effective operation of South Lanarkshire Leisure's computerised systems.
- Electronic communications are monitored automatically but normally this will not involve checking content. South Lanarkshire Leisure does however reserve the right to inspect the contents of any mails that are sent or received. The main reasons for monitoring are:
- To be in a position to block access to inappropriate or malicious content either sent or received by email.
- To monitor mail system capacity.

Reporting of email usage is carried out monthly. Monthly reports are produced and passed to the IT Business Officer. This report identifies each user and will summarise the number of internal and external mails sent and received. In addition ad hoc reports are produced as requested, for example by line managers who identify excessive usage by a member of their team.

These reports are retained for 6 months, as per the Data Protection Act, you are entitled to inspect the above log files. You can do this by asking your line manager or by contacting the IT Business Officer.

It may sometimes be necessary to check and process your email, for example if you are away from your desk for an extended period. This is to ensure that the Trust responds promptly to its customers and contacts.

If an individual computer is the subject of repeated problems an investigation of content and usage history may be carried out either by IT Services or by SLC's Internal Audit. For example if a users pc is repeatedly infected by computer virus programs a review of the emails accessed by that machine may have to be carried out.

4.6 Email good practice

This section offers practical advice on the use of email within South Lanarkshire Leisure. Note that training courses are available in the use of the email application Microsoft Outlook, for more information contact the IT Business Officer.

Some Common Questions and Answers

What should I do if I receive an e-mail from an unknown sender?

Users should be suspicious of all mail from an unknown source. Files obtained from sources outside the Trusts computer networks, including files attached to e-mails may contain dangerous computer viruses that could damage the Trusts computer network. Users should never open a file attachment in an external mail without first scanning the file with Trust-approved virus checking software. If you suspect any e-mail, do not open it, do not delete it and contact the IT Help Centre on 01698 45 5656 immediately.

What should I do if I receive an item of e-mail which should be responded to within a set period - for example a complaint, request for information from Councillor/M.S.P. etc.?

Correspondence should be recorded via appropriate mail logging in place and response prepared as normal.

When is it appropriate to use e-mail?

Users should be aware that while e-mail can be like a telephone call in its immediacy, it is still a written communication and is very easily printed out and even more easily passed on to many others. Although e-mails are not as formal as a letter or a memo they can and have been used as evidence in legal proceedings. Resources should formalise locally issues/business transactions which can be dealt with by e-mail. (Suggestions include routine requests for information, administrative arrangements, such as room bookings, meeting arrangements, circulating draft documents for comments etc.) Resources also need to ensure that employees are aware of the level of enquiry that they have the authority to reply to.

Why is it not allowed to send personal multimedia and audio files by email?

These files as well are often particularly large and unless prohibited can quickly take up large amounts of storage space and significantly slow down the performance of the system.

Why are some emails stopped by the Trust's email system?

Emails are all subject to scanning for inappropriate content and if anything is detected in an email that is either suspect or deemed in contravention of the Trust's policies it will be intercepted.

Content and Style

Remember that the recipient of any e-mail is an individual

Make sure that the tone or style of the mail is appropriate for the recipient

Make sure that you are the appropriate person to send the mail

Make sure that the content of the mail is accurate and that for any information provided:-

- That you have the appropriate authority to supply this
- That it does not breach any internal or external codes or legislation

External emails

When sending formal e-mails externally make sure these meet with the Corporate Standard for email, these are available on the intranet published by SLC's Corporate Resources.

- Create and use an e-mail letterhead where the message is on behalf of South Lanarkshire Leisure
- Keep it short, three lines should be enough. This can be included as part of your signature file or stored as an Outlook template,
- Create a signature file for consistency. Keep it short and concise. Include your e-mail address in case the signature gets separated from the header.
- Don't duplicate in your signature any material you have in your e-mail letterhead.
- External e-mails will automatically include a South Lanarkshire Leisure disclaimer notice.

The Message

Keep messages short, but do not let the meaning suffer. When replying, you will often be replying to only part of the received message, maintain the thread, but save space by not returning the whole of the original message, only the part to which you are replying

Attachments

Where possible, file attachments should be sent as shortcuts or hyperlinks- where mail is inter-departmental and the recipient has access to the area where the file is stored. These send the location of the file attachment, rather that a copy of the actual file.

- Important and relevant file attachments should be saved into appropriate file folders.
- Sending file attachments in external mail should be avoided if possible and agreed in advance with the recipient
- File attachments sent or received from external sources will be filtered by Trust virus checking procedures.
- All mail users should be wary of unsolicited mail and file attachments as these are increasingly how viruses are introduced into corporate networks
- If you have any doubt about the use of a file attachment, speak to your line manager and/or our IT Business Officer.

Privacy

If you send personal mail should include the word PERSONAL in the Subject header. You should encourage anyone sending you personal mail to adopt a similar approach.

When mailing to more than one external addressee, put the list of e-mail addressees in the BCC (Blind Copies) box to protect the privacy of your audience. Using the To or CC box lets all recipients see the full list of addresses

Make use of the Sensitivity message options to mark mail as confidential, private or personal as appropriate. Any mail marked as private cannot be further amended and will not be accessible to anyone you have given permissions to access your inbox.

Reading Mail

You should check your mail regularly, preferably three or four times a day and at least twice a day. If you are unable to check your mail, or if you are going to be out for more than a day, consider forwarding your email, giving someone else access to your mailbox and/or setting the out of office assistant to explain why you are unable to answer mail sent to you.

Mailbox

Each user is allocated space on the Exchange server for their mailbox - this includes the diary, contacts, inbox, sent items and all other folders and the contents of these folders. These folders start to fill rapidly and the storage area can be used up very quickly. File attachments in mail items are a particular issue and can use up valuable space.

All items in folders should be reviewed regularly and deleted or archived as appropriate. Mailbox items can be removed to archive mailbox files. Important file attachments or emails should be saved into relevant file storage areas. It is also possible to move and copy mail messages items into file folders.

Note: deleted items are retained on the Exchange server for 2 weeks.

Storage of email

E-mail messages are similar to other forms of communicated messages such as correspondence, memoranda and circular letters. Very few messages will need to be maintained online for a long period of time.

Email messages which do need to be retained as business records should be managed as per the guidance available from the IT Business Officer.

Each Resource should have a records retention policy for business records and documents, email messages that record business transactions or decisions should be included in this and managed accordingly. Advice on developing such a policy is available from the SLC's Archives & Information Management Service.

Sending Personal Data by Email

Occasionally there will be a need to send personal data by email, this may include information classed as either confidential or sensitive. Be aware that as part of the Data Protection Act we have a legal requirement to ensure that such information is secure. Inherently email traffic is not secure particularly emails sent to external organisations.

Always

- Be aware of the nature of the data to be sent and consider is there a more appropriate means of communicating.
- Check that the address correctly identifies the recipient.
- Ensure that the email is addressed only to those who have a specific need for that data.
- If available use the email options to identify the importance and sensitivity of the email.
- Consider sending sensitive information in a password protected file such as a Word document or Excel spreadsheet, bearing in mind the practical need to let only the intended recipients know the password.

Never

- Use any personal identifiers such as a name, address or NI number in the subject field.
- Send personal or sensitive personal data externally by email unless you can verify the email address is secure and they are entitled to receive this data.
- Send a password protected file and include the password in the body of the email instead inform the recipient of the password using another method of communication.

5. DATA HANDLING PROCEDURES AND USE OF REMOVABLE MEDIA

5.1 General principles – data handling

This code of practice applies to you if you have access to or make use of any of South Lanarkshire Leisure's information. Any inappropriate use of South Lanarkshire Leisure's information may lead to action as defined under South Lanarkshire Leisure's disciplinary procedures.

It is important that you read this code of practice carefully. If there is anything that you do not understand, please discuss it with your line Manager or IT Business Officer.

This policy recognises the value and importance of information but also the threat presented by the loss of removable media that could hold large data sets of either personal or sensitive data.

The Trust's information assets should routinely be stored and accessed from its network location where it is physically secure and is routinely backed up. Removing Trust information from its network location should not be considered unless there is a valid business case for doing so.

Before any transaction is undertaken using such information the risk of losing this information must be considered and if necessary appropriate precautions enforced. For advice on how to complete information security risk assessments contact the IT Business Officer.

Unless there is a valid business case agreed and authorised by your manager:

- Removable media should not be used to replace network storage.
- Trust data should not be left unencrypted if it is to be taken outside the normal location of that information.
- Trust data should not be left unencrypted if it is to be left unattended by an authorised user of that data.

5.2 Removable media risks and acceptable use

There will be occasions when there is a valid business case for using removable media, such as USB memory sticks, external hard drives, CD Roms etc. however it has to be recognised that the use of these devices also carry with information security risks and the use of these devices must be authorised by your manager.

It is only acceptable to use removable media for the following reasons:

- Retain a temporary copy of an individual record to allow work to be done remotely. If this is done the temporary copy must be returned to network storage and the temporary copy destroyed as soon as possible.
- In exceptional circumstances create a copy of a complete file or data set to enable work to be completed either off site or by a third party.
- As part of a partnership arrangement with other public authorities if no more secure transfer arrangement can be made.

The ease with which these devices can be used to hold and transport large amounts of data present risks to valuable data assets that include the following:

- Inadvertent loss of complete data sets if the device is mislaid or lost in transit.
- Malicious or deliberate theft of complete data sets by individuals with access to the network.
- Recognising this IT Services have defined a set of controls that are to be applied when using these devices.

SLC's IT Services maintain a list of devices that can be used as removable storage devices. Note if they are to be used to store sensitive information or data any such files placed on a device must be protected from unauthorised access by encryption. Encrypted memory devices are available and should be used whenever se

If and when removable media is used physical security best practices must be followed to prevent the theft or loss of removable media and data. Users often leave removable media in lab computers or, because of their small size, simply misplace them.

Table showing acceptable uses of removable media

Use	**Risk**	**Information security controls**
Individual record copied to allow off site or remote working	Inadvertent loss	Record must be password protected or an encrypted memory device used. Line manager must be informed and authorisation given.
Complete file or dataset taken off site.	Inadvertent loss, malicious access	Risk Assessment completed. Device and file must be encrypted. Line Manager or IT Business Officer informed and authorisation given.
Dataset prepared for data sharing partnership	Inadvertent loss, Malicious access	Risk Assessment completed. Partnership protocol followed but as a minimum device and file must be encrypted. Line Manager or IT Business Officer informed and authorisation given.

For advice or guidance on how to use portable devices or media please contact the IT Helpdesk or our IT Business Officer.

Trust Telephone Systems

5.3 General Principles of phone use

This section provides guidance on the use of telephones provided by the Trust including mobile phones and similar handheld devices.

Employees who make use of Trust supplied mobile phones will be asked to record their acceptance of these conditions when the device is issued to them.

Guidelines for the acceptable use of telephones

Telephone calls should be kept as short as possible.

Telephones are provided for use in support of Trust business.

The telephone handset and associated accessories are the property of South Lanarkshire Leisure and should normally be used for legitimate Trust business purposes only.

The Trust's corporate telephone network provides free calls between HQ and SLC primary offices, using a number of tie line prefixes. Extensions in offices on the corporate network can be called by dialling the tie line prefix followed by the extension number. The tie line codes are listed below.

Tie Line Prefix	Sites In Tie Line Area [1]
810	South Vennel, Lanark Business Unit (8107)
811	Carluke Housing Office
812	Accies Stadium
813	Almada St., Montrose House, Brandon Gate, Townhouse, Caird St. data centre, Calder House, High Patrick St., John St.. (Blantyre), Pollock Avenue, Larkhall Housing Office
814	Lindsay House
815	Forrest St.
845	Rutherglen Housing Office
846	Cambuslang Housing Office
847	Rutherglen, King St.
848	Cambuslang Q&A
849	Rutherglen Business Unit

Calls between sites attached to the corporate telephone network should **not** be made over the public telephone network since such calls are chargeable.

Users **must not** use, try to use, or let anyone else use Trust-supplied telephone equipment for:

- Anything that is illegal or immoral
- Making offensive or threatening calls
- Making calls which can be construed to constitute harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, or political beliefs
- Unreasonable personal use
- Use in relation to any other business owned or operated by the user

It may be necessary from time to time for a user to make a personal call using a Trust telephone line. Where possible, prior permission to do so should be sought from a line manager. Users may be required to identify

[1] Note that it is not necessary to dial the tie line prefix when calling extensions within the same tie line area.

such personal use from the associated monthly billing report, and may be expected to pay for this use at the relevant tariff. This approach has been agreed with SLC's Internal Audit and SLC Corporate Personnel. Inland Revenue guidance indicates that no personal tax liability results from the personal use of business telephones other than the payment of VAT on call charges.

Internal telephone extensions and landlines **should not** be diverted to mobile telephone numbers unless there is no alternative - diverted calls incur considerable charges. Voicemail can be provided on all fixed telephone lines.

You should take precautions to avoid revealing sensitive or confidential information to unauthorised personnel from being overheard by unauthorised personnel in your immediate vicinity or close to the person with whom you are talking.

You should take steps to confirm the identity of the person to whom you are talking and establish the security of their location before discussing sensitive or confidential information. Such information should never be passed on by leaving a message on an answering machine.

The monthly billing summary from SLC of all calls made from each handset, supplied to billing coordinator within the Trust, includes details of all call activities.

Users have a responsibility to utilise the Trust's communications resources and services in a manner that is consistent with the Trust's standards of business conduct, as described in the Trust's Code of Conduct for Employees.

Voicemail

Voicemail and answering machines can be made available to employees at the request of line management based on individual job requirements.

Voicemail messages are Trust records. The Trust reserves the right to access the contents of these messages if there is reasonable cause. Employees will be advised, if possible, when this is to happen. It should not be assumed that voice mail messages are private or confidential. Such access may be required in searches for lost messages, to comply with investigations into wrongful acts or to recover from system failure.

Personal use of voice mail by employees is permitted but should not interfere with, or conflict with, the employee's work. Personal messages will be viewed in the same way as other messages since they cannot be identified as personal.

Since personal messages may be accessed by managers without prior notice, voicemail should not be used to store messages that are not be heard by a third party.

Non-personal voice mailboxes can be setup when necessary and access provided to employees as required. A nominated user must be assigned responsibility for the mailbox.

Employees are responsible for maintaining the security of their voice mail. Employees should take precautions to prevent unauthorised access to their mailbox by ensuring their access pin code number is not divulged to personnel not authorised to use it.

Unauthorised entry to another employee's voice mailbox is not permitted. The default setting for a mailbox will permit access for the user only. The user may permit other users to access the mailbox, as required. Any other

access will be permitted only with the authorisation of the user's line management or the IT Business Officer.

Users are responsible for maintaining their mailboxes. Voicemail should normally be checked at least daily. Voicemail messages should not be stored for longer than is necessary. Mailbox greeting messages should be kept current, accurate and relevant.

Privacy

Telephone usage is subject to routing monitoring and auditing. All outgoing telephone calls are logged and can be traced by the phone provider this function can be invoked at any time should misuse be suspected.

Unexpected peaks and apparently excessive usage may be investigated in conjunction with the relevant line managers.

The IT Business Officer has online access to detailed call history data for each phone line or extension under their administrative control and can generate reports showing details of individual calls.

Given that telephones are provided for Trust business use, there should be no expectation of privacy. However, it is recognised that communications systems are a vital part of the operation of the Trust and are critical to service provision. To ensure effective and efficient use of its Communications systems the Trust will:

- Attempt to preserve the privacy of personal communications.
- Not access the contents of any communication without reasonable cause and will advise employees, if possible, when this is to happen.
- Monitor the amount of traffic generated by its communications systems, wherever required, to ensure that they operate efficiently and are not subject to misuse.

The Trust reserves the right, subject to the points above, to intercept, record and disclose as necessary calls made or received on its telephones and telephone systems without regard to content, as part of investigations into systems failure, potential wrongdoing or criminal acts, or for training purposes.

The Trust will not record telephone calls for any other purpose without informing all affected employees and including an appropriate notification message at the start of every recorded call.

Health & safety

While there are no particular risks associated with the normal use of telephone systems, bacteria and germs can gather on handsets, especially those used by many people. Cleaning kits are available from the purchasing section in each facility. It is recommended that phones are cleaned on at least a monthly basis.

Care should be taken to ensure that telephone cords are not stretched, run across the floor, or positioned in any way as to create a risk of tripping, falling or personal injury.

Most basic telephones are powered by a low voltage electrical supply on the cable, but some telephones and accessories are powered by mains electricity. Normal safety precautions should be observed when handling these devices, and they should be submitted for annual Portable Appliance Testing, in line with Trust policy.

All telephones, systems and accessories must be used strictly in accordance with the manufacturers' guidelines as supplied with each device.

5.4 Mobile Communications Devices

Mobile phones and any other mobile communications devices are provided for use while on Trust business. Mobile telephone calls are often more expensive than fixed line calls, and so they should be kept as short as possible. They should only be used where no fixed alternative telephone line is available, or where the use of a fixed line is inappropriate.

In particular, Trust mobiles **should not** be used to make calls from within Trust offices – internal calls, made between HQ and SLC are via a private telephone network, are free, and calls from all Trust fixed lines to mobiles and other fixed lines are charged at a lower rate than similar calls from mobiles.

The mobile device is the property of South Lanarkshire Leisure and should normally be used for legitimate Trust business purposes only. However, it may be necessary from time to time to make a personal call or send a personal text message. You will be required to identify such personal use from the associated monthly invoice, and will be expected to pay for this use at the relevant tariff, by means of petty cash payment, internal invoice or direct salary deduction. This approach has been agreed with SLC's Internal Audit.

Communications devices capable of transmitting and receiving data information, such as Personal Digital Assistants and certain mobile phones, should only be used for the purposes for which they were supplied. They **must not** be connected to third party networks or directly or indirectly to the public Internet, unless previous authorisation to do so has been received from the relevant line manager and the IT Business Officer. This will ensure that these devices remain free of viruses or other malicious software that may be transmitted on unknown networks.

You **must not** use, try to use, or let anyone else use Trust-supplied mobile communications devices:

- To send or receive inappropriate or offensive remarks, graphics or images
- In contravention of Regulation 104 of the Road Vehicles (Construction & Use) Regulations, 1986; i.e. using a mobile phone whilst driving

The sending or receiving of SMS text messages for the purposes of downloading or otherwise accessing ring tones, games, commercial competitions, sports services and other non-business related activities or applications is **not permitted**. It should be noted that many of these services operate on an on-going subscription basis. Users should not send SMS text messages to chargeable services without the authority of their line manager.

Users have a responsibility to utilise the Trust's communications resources and services in a manner that is consistent with the Trust's standards of business conduct, as described in the Trust's Code of Conduct for Employees.

When visiting non-Trust sites, you should be aware of and respect local policies regarding the use of mobile communications devices. For instance, it may be necessary to switch such devices off in Hospitals, Courts etc. If in doubt, local employees will be able to describe local policies.

Mobile phones supplied to the Trust are, by default, barred from making international calls or calls to the UK from abroad. These restrictions can be lifted for individual phones, for instance where there is a need to contact counterparts in foreign countries or to contact employees attending conferences etc. outside the UK. Where International access is required, users should seek authorisation from their line manager who should contact the IT Business Officer, providing details of the phone number concerned and the start and end dates of the requirement.

Trust-provided mobile communications devices may only be used by designated users. Where such devices are capable of accessing the Internet or the Trust's email system, the Trust's Email and Internet Usage Policy applies - you should be aware of your responsibilities under this Policy and in particular should note the Trust's policy relating to passwords and ensure that the password associated with the device is known only to you and not divulged to any unauthorised person.

A number of phone handsets incorporate digital cameras. Such devices can offer a cost-effective alternative to separate handsets and cameras for those users who need to capture digital images. However, such use can pose a risk to security and privacy, particularly in sensitive locations such as schools and areas open to service users. If you need to use a camera phone, you should respect local rules defining their use, and always be sensitive to the privacy of others. If in doubt regarding the acceptable use of camera phones, you should consult the site manager. Note that the software supplied with such devices should not be installed on a Trust PC without prior permission from the IT Business Officer.

Monthly, itemised invoices are produced in respect of each phone number. These are provided to the IT Business Officer.

Calls from mobile phones are logged and can be traced by the network operator; this function can be invoked at any time should misuse of a handset be suspected.

Malicious calls, mobile spam and marketing

Should you receive a call on your mobile phone that is offensive, malicious or otherwise unacceptable, you should follow the procedure described below:

- If possible, simply ignore the call. You are in control of the calls you receive.
- If you do receive an unacceptable call, end it as soon as possible and immediately contact the Vodafone malicious call reporting service by dialling **191*** from your mobile handset – an agent will note the last call made to your phone as having been unacceptable. Don't delay dialling 191* till another call is received.
- Record all supporting evidence of the call – date, time, calling number, contact name, company details etc. This makes any subsequent investigation much easier to perform.
- Contact the IT Help Centre to report the issue.
- If the nature of the call was such that an illegal act was committed, contact the Police.

The Trust's mobile phones are registered with the Telephone Preference Service, which means that you should not receive unsolicited marketing and sales phone calls. Any such calls you do receive may be in contravention of the code of conduct imposed upon service operators by the telephone regulator, OFCOM. In the event that you receive such a call, you should contact the IT Help Centre with details of the time, date and phone number, and any relevant contact or company details provided by the caller. The IT Networks section will report the matter.

Should you receive unsolicited SMS text messages, known as "spam", from unknown sources, you should not act upon or reply to them – unscrupulous operators have been known to use sophisticated methods to generate calls to Premium Rate or other chargeable services. In such cases, you should send a Text saying **Stop** to the source number – the service is then obliged by the terms of its OFCOM license to cease sending messages to your number. If in doubt, contact the IT Help Centre.

The Vodafone offers a spam monitoring and reporting service called VSPAM. Should you receive a spam text message, you should forward the message to VSPAM on 87726. If you continue to receive unsolicited texts, you should report the matter to the IT Help Centre.

Mobile devices and driving

The Highway Code and the Council's Driver Handbook make it clear that drivers should **never** use a hand-held mobile phone and that using a hands-free phone is likely to distract a driver's attention from the road.

In light of the above, mobile communications devices **should not** be used while driving any vehicle while it is in use on Trust business. Further, **any** mobile communications device should be used in a manner that complies with the law at **all times -** on all occasions, you **should find a safe place to park and switch off the engine** before using any such device while driving a vehicle.

Should you have an accident while using a mobile phone when driving on Trust business, you should note that your private motor insurance will be expected to meet the costs of damage repairs and any personal injury claim that may arise.

Security of mobile devices

Mobile communications devices should be securely stored when not in use.

Handset covers provide a degree of physical protection and can be provided with mobile handsets. You may be liable for repair or replacement costs should your handset be damaged or lost. Such matters should be reported to your line manager, and to the IT Help Centre.

The loss of devices that can send, store and retrieve email or access Trust information systems (including Blackberry® handhelds and certain mobile phones) has potentially serious repercussions for the Trust because of the sensitivity of the information that may be stored on them.

Sensitive, confidential or otherwise valuable information **should not** be stored on mobile communications devices; such devices **should not** be connected to Trust computer systems without prior discussion with the IT Business Officer.

Any loss of mobile communications devices **must** immediately be reported to the IT Help Centre, who will arrange to have it permanently disabled. If the loss is discovered out of hours, it **must** be reported to the Vodafone Customer Services (**08700 711 102)** who will immediately disable the device such that it cannot be accessed or used by anyone else. The IT Help Centre should be contacted as soon as possible within working hours to report the loss, in order that delivery of a replacement handset can be arranged. Failure to report loss or theft of handsets may result in liability for charges subsequently incurred using it.

Health & safety

Mobile phones are small, low power radio frequency transmitters and are designed to operate within electromagnetic exposure guidelines to safeguard public health. A Government body, the National Radiological Protection Board (NRPB), sets these guidelines. In response to media speculation surrounding possible health effects, the NRPB issued a statement in March 1999, stating:

"…At present, the international consensus in the worldwide scientific community is that there is no demonstrable health risk. If any of the scientific work being carried out in the UK, EU countries, the USA or elsewhere, indicates a health risk from the use of mobile phones, the NRPB will review its advice".

Press and media speculation regarding the possible damaging effects on health of prolonged use of mobile telephones has persisted for a number of years. To date, no clear evidence has been published in support of claims of adverse health effects. In May 2000, the Independent Expert Group on Mobile Phones (The Stewart Report) reported that:

"…The balance of the evidence available does not suggest that RF (Radio Frequency) radiation from mobile phones or base stations causes cancer or other brain diseases. However, there is now evidence that effects on biological functions, including those of the brain, may be induced by RF radiation at levels comparable to those associated with the use of mobile telephones. There is, as yet, no evidence that these biological effects constitute a health hazard, but at present only limited data are available. This is one reason why we recommend a precautionary approach."

Recent coverage in the media focused on potential effects of the use of mobile phones by children, and concluded that, if negative long-term health effects do result, they are likely to affect young children first and most seriously[2]. The available advice is that mobile phones should not be used by children under eight. Notwithstanding that, Trust mobile phones should **never** be used by children.

Some reports suggest that using mobile phones via personal hands-free devices may reduce the amount of radiation delivered to the head, because the transmitter is held further away from it. Vodafone, the Trust's mobile network supplier, firmly recommends the use of hands free kits. The Trust provides these as standard equipment with all handsets.

Repeated and / or prolonged use of mobile phones should be avoided, and hands-free kits should be used at all times. Mobile phones **must not** be used while operating machinery of any kind.

[2] http://news.bbc.co.uk/1/hi/health/4163003.stm