Livewell Southwest

Communication Systems (Phone, Email, Internet & Fax) Policy: Usage and Equipment

Version No 1:4

Review: May 2019

Notice to staff using a paper copy of this guidance

The policies and procedures page of LSW intranet holds the most recent version of this document and staff must ensure that they are using the most recent guidance.

Author:	**PICTS and Information Governance Group**
Asset Number:	**820**

Reader Information

Title	**Communication Systems (Phone, Email, Internet & Fax Policy): Usage and Equipment. V.1.4**
Asset number	820
Rights of access	Public
Type of paper	Policy
Category	Non Clinical
Document purpose/summary	This policy covers and regulates use of phone, email, internet and fax usage and equipment by all LSW staff.
Author	Information Governance Group
Ratification date and group	9th May 2016
Publication date	12th May 2016
Review Date and Frequency of Review	12th May 2019 The Policy Ratification Group will retain an e-signed copy for the archive in accordance with the Retention and Disposal Schedule, all copies must be destroyed when replaced by a new version or withdrawn from circulation.
Disposal date	The PRG will retain an e-signed copy for the archive in accordance with the Retention and Disposal Schedule, all copies must be destroyed when replaced by a new version or withdrawn from circulation.
Job title	Information Governance Lead
Target audience	All staff employed by Livewell Southwest
Circulation list	Electronic: Livewell Intranet and LSW website Written: Upon request to the Policy Ratification Secretary on ☏ 01752 435104. Please note if this document is needed in other formats or languages please ask the document author to arrange this.
Consultation process	Information Governance Group, Plymouth Information Communication Technology Shared Service (PICTS), Joint Trade Union Forum (JTUF), Joint Committee for Consultation and Negotiation (JCCN), District Nurses Forum, Inpatient Professional Nurse Forum Policy Ratification Group, Workforce Policy Group
Equality analysis checklist completed	Yes
References/sources of information	• The Common Law Obligation of Confidentiality • The Data Protection Act 1998 • The Computer Misuse Act 1990 • The Access to Health Records Act 1990 • The Copyright, Designs and Patents Act 1988 • The Public Records Act 1958/1967 • The Human Rights Act 1998

	• The Crime and Disorder Act 1998 • The Regulation of Investigatory Powers Act 2000 • The Freedom of Information Act 2000 • The Caldicott Committee Report on the Review of Patient-Identifiable Information Report • NHS IM&T Security Manual – NHS Information Authority • BS7799 • The Protection and Use of Patient Information – Department of Health
Associated documentation	• IT Security Policy • Information Governance Policy • Incident Reporting & Investigation Policy • Disciplinary Policy • Security Policy • Safe Haven Policy • Confidentiality Policy • Audio-visual Recordings of Patients/Visitors/Staff and Business Activities Policy
Supersedes document	All previous versions
Author contact details	By post: Local Care Centre Mount Gould Hospital, 200 Mount Gould Road, Plymouth, Devon. PL4 7PY. Tel: 0845 155 8085, Fax: 01752 272522 (LCC Reception).

Document review history

Version no.	**Type of change**	**Date**	**Originator of change**	**Description of change**
0.1	Draft	13/07/12	A Saxby	New document
0.2	Draft	23/07/12	A Saxby	Comments from IGG
0.3	Draft	10/08/12	A Saxby	Comments from IGG
0.4	Draft	15/08/12	A Saxby	Comments from consultation
0.5	Draft	09/10/12	A Saxby	Comments from JTUF
0.6	Draft	20/11/12	Workforce Policy Group	Further comments from Workforce Policy Group
1.0	**Ratified**	**19/12/12**	**JCCN**	**Minor amendments**
1.1	Updated	16/01/13	A Saxby	Reader sheet
1.2	Minor amend	04/06/14	A Saxby	Para. 7.4.5 added.
1.3	Minor amend	19/09/14	A Saxby	Section 8.4.1 amended
1.4	Minor Amend	01/05/16	C Batten	PCH changed to LSW Updated SIRO Information Added 7th Caldicott Principle

Contents		Page
1	Introduction	6
2	Purpose	6
3	Definitions	6
4	Duties & responsibilities	6
5	Equipment Security and Passwords	7
6	Systems and Data Security	8
7	Phone usage	9
8	Email usage	13
9	Internet usage	17
10	Fax usage	20
11	Mobile computing devices	22
12	Training	26
13	Monitoring compliance and effectiveness	26
Appendix A	Request for Livewell Southwest to contact patient via personal email address	28
Appendix B	Example fax cover sheet	29
Appendix C	Quick reference guide	30
Glossary		32

Communication Systems (Phone, Email, Internet & Fax Policy): Usage and Equipment

1 Introduction

1.1 Our Information Technology (IT) and communications systems are intended to promote effective communication and working practices within our organisation. This Policy outlines the standards you must observe when using these systems, the circumstances in which we will monitor their use, and the action we will take in respect of breaches of these standards.

1.2 In particular, remember that you are representatives of Livewell Southwest (LSW) and all communications through our systems (whether by phone, email, internet or otherwise) must be conducted in an appropriate manner. It is important that they are used responsibility, are not abused, and that individuals understand the legal, professional and ethical obligations that apply to them.

1.3 This Policy covers all employees working at all levels and grades. It also extends to persons working for LSW such as secondees, agency staff, volunteers, contractors and others employed under a contract of service, and all other individuals using or accessing LSW services and equipment whether on or off site (collectively referred to as **staff** in this Policy).

1.4 Phone and computer network services and resources are corporate assets. The use of equipment and services is limited to work related purposes, except when approved in writing by a director, locality manager and head of department.

2 Purpose

2.1 This Policy deals mainly with the use (and misuse) of phones, email, internet and fax and to make users aware of what LSW deems to be acceptable and unacceptable. Misuse of IT and communications systems can damage the business and reputation of LSW.

3 Definitions

3.1 See Glossary.

4 Duties and responsibilities

4.1 LSW and its staff have a legal obligation to comply with the Office of Communications (OFCOM) regulations, the Computer Misuse Act, and other relevant policies such as LSW's Information Governance Policy and IT Security Policy.

4.2 Plymouth Information Communication Technology Shared Service (PICTS) provides ICT support and services to LSW. They have a corporate responsibility for the management, maintenance and support of the telecommunications and computer network infrastructure (telephone exchanges, wiring, all telephone extensions and computer network equipment).

4.3 The staff within PICTS act as the delegated agents of the Chief Executive and are responsible for maintaining a safe and secure computing environment in LSW. More specifically they are responsible for ensuring that the LSW conforms to the NHS Statement of Compliance and have fully implemented the NHS Security and Access Policy.

4.4 **Managers/Team Leaders** - All managers and team leaders have a specific responsibility to operate within the boundaries of this Policy and ensure compliance with the policy within their areas of responsibility.

4.5 **Staff** – All staff are responsible for the success of this Policy. Staff should behave in a safe and responsible manner, taking steps to reduce the risks that can be associated with the use of mobile phones, email, internet etc. All staff must immediately inform their line manager of any incident which is considered to be a significant risk, and promptly report all incidents (including near misses) via LSW's incident reporting system.

4.6 All staff must comply with this policy at all times. Breach of this policy will be dealt with under the Disciplinary Policy and, in serious cases, will be treated as gross misconduct leading to a Disciplinary Panel and the Panel would have options available to them up to and including dismissal from employment.

5 Equipment Security and Passwords

5.1 The purchase of all communication devices, computer network equipment and services must be requested through PICTs and will require prior approval from the Director of Finance.

5.2 Staff are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy.

5.3 Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else.

5.4 If leaving a desktop computer/mobile communication device unattended or on leaving their normal place of work staff should ensure that they lock their computer/mobile communication device or log off to prevent unauthorised users accessing the system in their absence. Staff without authorisation should only be allowed to use desktop computers/mobile communication devices under supervision.

5.5 Staff who have been issued with mobile communication devices e.g. laptop, Smartphone, must ensure that it is kept secure at all times to ensure that they are not damaged, lost or stolen, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Staff should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

5.6 Only equipment intended for the purposes of mobile communication and working is authorised to be taken off LSW premises unless there is documented managerial approval. Any equipment located in easily accessed areas should be physically secured and rooms should be locked when not in use.

5.7 If a mobile phone is lost or stolen, it is the responsibility of staff to ensure that a bar is immediately placed on outgoing calls via the PICTS Service Desk on 437000 (int. 37000). The loss or theft of a portable device must immediately be reported to the line manager as well as the Local Security Management Specialist in the Risk Management Department. The incident reporting procedure should be followed as loss/corruption of data could potentially be a series incident requiring investigation and would need to be investigated immediately.

5.8 Negligence in the care of portable devices or failure to report loss or damage at the earliest opportunity may be subject to LSW's Disciplinary Policy.

5.9 Any suspected phone security violations (relating to inappropriate use of mobile phones, internet, email, fax etc) should be brought to the attention of PICTS, LSW's Local Security Management Specialist, or the Information Governance Team who will investigate and record the incident in accordance with the Incident Reporting and Investigation Policy.

5.10 PICTS actively monitors the network for capacity management and to prevent abuse. Periodic and random monitoring of telephone usage and length of calls will take place for audit, fraud monitoring and engineering purposes. Phone call information, such as date, time, duration, dialled digits etc., is continually recorded. Internet and email services are also audited in order to monitor inappropriate use.

6 Systems and Data Security

6.1 Staff should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk.

6.2 Staff of computer network devices will only be granted access to the systems that are appropriate for their role. Appropriate usage guidelines are outlined in this Policy and in LSW Information Governance policies.

6.3 Only LSW owned computer and phone devices can be used to connect to data and phone networks e.g. group drives, telephone directory, network resources etc. However, NHS mail can be accessed via privately owned computers and phone devices, and guidance is available from NHSmail.

6.4 For financial control purposes, LSW phone lines will only allow the minimum practical and appropriate access level (i.e. internal/site wide, local, national). There will be no international access unless specifically approved by the Director of Finance.

6.5 To ensure an optimum quality of service, all communication systems and computer network device related issues, problems and faults must be reported through the PICT Service Desk, on 437000 (int. 37000).

7 Phone usage

7.1 Private Calls and Charging

7.1.1 Private calls are those which are made for personal reasons, and **not** connected with LSW business.

7.1.2 All private calls made from desk phones must be identified as such and paid for by staff. You can do this by contacting LSW's Switchboard Private Call Docket system. An administration surcharge of 20p is levied in addition to the call charge. LSW issued mobile phones are covered differently via the Fair Use Policy covered in Section 7.5.2. In exceptional circumstances, e.g. if asked to work longer/later than usual, staff may call home to notify their family having first gained the approval of their line manager or nominated representative.

7.1.3 Please also refer to 4.6 and 5.9 regarding the Acceptable Use of Phones.

7.2 Reverse Calls

7.2.1 LSW staff must **not** accept reverse charge calls, however there may be exceptional circumstances where this may arise. In this event priority authority should be sought by the PICTS Technical Services Manager, a nominated representative or your line manager.

7.3 Home telephone line rental reimbursement for on-call staff

7.3.1 On-call staff cannot claim for reimbursement of their home phone line rental costs, but may have use of a LSW mobile phone whilst on-call. LSW provided mobile phones will only be allocated to essential users and only one mobile will be allocated per on-call rota.

7.4 Obtaining a mobile phone

7.4.1 LSW staff who need a mobile phone must first gain the approval of the relevant budget holder and meet one or more of the justification criteria including:

- Mobile phone is be used for out of hours, off site, on-call duties and shared between staff covering the on-call duty; and/or
- Mobile phone is to be used for Health & Safety i.e. lone working (please refer to the Lone Work Policy on the intranet) or physical security purposes for community based staff; and/or
- There is a requirement for an individual to be contactable whilst working away from their normal place of work and where other methods of communication are unsatisfactory.

7.4.2 All purchase, maintenance and ongoing costs will be invoiced to the department ordering the equipment.

7.4.3 Mobile phone equipment may only be rented from Vodafone, although if there is a requirement an order can be made from Orange. Maintenance is provided by the supplier whilst under initial warranty and at extra cost thereafter. Fault repair/replacement is arranged by PICTS.

7.4.4 Mobile phones remain the property of LSW and as such must be disposed of via PICTS. Leavers must return their mobile phone to PICTS for cessation or re-allocation. Failure to comply with this policy will result in the user being invoiced for the full cost of the modern equivalent handset and any other associated costs. A replacement handset is approximately £72.

7.4.5 ‘LSW work mobiles are another method for people who use our services to contact staff when they are working remotely, mobile working, at another location etc. The same principles would apply to services when they provide other contact details e.g. landline, email etc.’

7.5 Personal use of LSW mobile phones

7.5.1 A ‘fair use’ policy is implemented within LSW in respect of personal calls/text messages from LSW mobiles. If staff need to use their mobile phone for personal use they must make a request to the ICT Telecoms Team (plh-tr.telecomsbilling@nhs.net), copying in their line manager and stating their requirement and employee number. They will then have a monthly salary deduction of £10 set up to cover personal calls/text messages. Users are expected to monitor their own personal usage every month to ensure it does not exceed the £10 personal allowance.

7.5.2 Mobile use activity is monitored both by the ICT Telecoms Team and Counter Fraud and any personal use not accounted for, or any use over the £10 per month threshold must be communicated to the Telecoms team.

7.6 Premium/international calls from mobile phones

7.6.1 Premium/international calls will be barred by default. This bar can be lifted for specific periods on approval from the Director of Finance by emailing PICTS, providing the mobile number and dates, and giving at least five working days notice.

7.7 Restrictions on use of mobile phones

- **Within LSW premises:** Due to the potential for interference with electronic medical equipment, mobile phones must not be used within two metres of any electronic medical equipment in any area of LSW. Clinical staff, in the course of treating patients, may use their LSW mobile phones in clinical and ward areas providing it is not within two metres of any electronic medical equipment. They should be used only when it is absolutely necessary, and wherever possible, land lines should be used instead.

    - Staff should be aware of their surroundings when using mobile devices, especially when discussing confidential information.

    - Mobile devices should be kept on silent during meetings, training courses etc.

- **Mobile telephone cameras/recorders:** Mobile phone cameras must not be used in any patient areas for quality, privacy and confidentiality reasons. Staff are asked to be vigilant in bringing this policy to the attention of other staff, patients and visitors.

- **Whilst driving:** For safety reasons, LSW staff **must not** use a mobile phone whilst driving any vehicle (unless it is hands free). Staff must pull over at the earliest opportunity, when and where safe to do so and switch off the engine to make or return a call. No in-car mobile phone kits will be provided by LSW. LSW **will not take responsibility or be liable in any way** for someone charged with using a handheld device whilst driving and will not in any circumstances contribute in any way to the payment of fines or other expenses incurred by use of a handheld device except for those costs detailed in this policy.

7.8 Acceptable use of mobile phones

7.8.1 Staff may use their mobile phones in non-clinical areas such as offices, main corridors, the main concourse, shops, restaurants, foyers, waiting rooms, etc.

- Staff should not make or receive personal phone calls from LSW or personal mobile phones at times which affect the operational service of their department.

- Personal mobiles must be switched off in all clinical and ward areas.
- Personal mobiles should be on ‘silent’ ring tone at all times to avoid disturbing others.

7.9 Services using Short Message Service (SMS)

7.9.1 SMS or text messaging is an attractive technology for quick communication of short messages and is a widely accepted form of communication. LSW encourages the use of SMS for simple transactions such as appointment reminders to help reduce non-attendance. The following **guidelines** should be adhered to when using SMS for appointment reminders.

- Staff sending a SMS should use NHSmail, where this facility is provided.
- SMS messaging must **not be used for sensitive personal information** such as test results or discharge summaries. It must be used only for appointments and other non sensitive information.
- The recipient must consent to LSW using their mobile phone number for this purpose - this could be achieved at the time of recording a mobile phone number.
- A record of consent **must** be recorded as agreed in local protocols e.g. SystmOne
- The recipient may withdraw their consent to receive SMS messages at any time by informing the relevant service/health professional.
- The sender must be sure that the phone number being used is that of the intended recipient (i.e. the ‘safe haven’ principle) as phones are regularly changed, exchanged or sold.
- It is good practice to regularly re-confirm the service user’s mobile phone details, e.g. when attending an appointment.

SMS example:

This is a reminder for your appointment tomorrow. Please telephone XXXXX if you are unable to make your appointment, thank you.

Note extract from NHSmail Acceptable Use Policy:

> *‘4.1.10. If using SMS as an alerting or notification system you should ensure you have carried out a relevant risk assessment in relation to the limitation of SMS, particularly its insecure nature and lack of delivery guarantee and delivery notifications. It is not recommended for use where personal data is exchanged or guaranteed delivery is required.’*

7.10 Security

7.10.1 Where mobile phone mailboxes are used, any associated passwords/Personal Identification Numbers (PINs) must be changed from the service provider’s default.

Good practice for password security should be followed. Further advice is available from PICTS.

7.10.2 Staff must observe their responsibilities in conjunction with the Data Protection Act when storing phone numbers and personal information on mobile phones. Staff issued with a Smart Phone should refer to the LSW Information Security Policy for data protection guidance.

7.10.3 In the interests of security, PICTS must mark all new mobile phones before issue.

8 Email usage

8.1 Email is a vital business tool, but an informal means of communication, and should be used with great care and discipline. Staff should always consider if email is the appropriate method for a particular communication. Messages should be concise and directed only to relevant individuals.

8.2 Email etiquette and content

8.2.1 Staff should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff should assume that email messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain. Examples include:

- If you send or forward any emails with any libellous, abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate emails.
- If you unlawfully send or forward confidential information **you** can be held liable under the Data Protection Act 1998.
- If you unlawfully forward or copy messages without permission **you** can be held liable for copyright infringement.
- If you negligently send a virus or file containing a virus **you** can be held liable.
- If you forge or attempt to forge email messages.
- If you send an email from another persons email account.
- If you disguise or attempt to disguise your identity when sending mail.
- Where an email constitutes a clinical/corporate record it must be filed with the relevant records and not kept in an individual’s mailbox.

8.2.2 Good practice

- Always enter a suitable description in the subject line.
- Writing emails in capital letters could be considered as shouting.
- Delete emails that they do not need to retain.

- Do not send or forward chain mail, junk mail, jokes, gossip or other frivolous material.
- When receiving emails beware of the possibility of receiving viruses and ensure that your antiviral precautions are up-to-date.
- When sending large attachments compress documents using suitable software.
- Use large distribution lists sensibly and appropriately.

8.2.3 Use of this service for illegal activity is grounds for immediate dismissal, and LSW will, without exception, always refer any such incidents to the police. Illegal activity includes (but is not limited to) material related to paedophilia, terrorism, incitement to racial harassment, stalking and sexual harassment and treason. Suspicion of such activity may be referred to the appropriate body for their investigation.

8.2.4 Staff shall not send defamatory material by email, or send communications which knowingly cause distress or offence to another user, or transmit any files of an obscene or pornographic nature. The transmission of any kind of sexually explicit image or document using this service is expressly forbidden. If you need to transmit sexually explicit images or documents for a valid clinical reason, then you shall obtain the permission of the local Caldicott Guardian and inform the Information Security Team that you intend to use the email system for this purpose before you start doing so.

8.2.5 Staff shall not attempt to introduce computer viruses via email messages or attachments. The deliberate or negligent transmission of any virus, worm, "Trojan", trap-door or other malware programme code using this service is expressly forbidden. NHS Connecting for Health will seek reasonable compensation through LSW in the event that any of your activity causes any detriment or loss of any kind to the national network service.

8.2.6 Staff shall not attempt to send persistent email communications to an individual or mailing list when, as a result of any complaint, a warning has been issued that further communication are not wanted.

8.4 Confidential data exchange and person identifiable information

8.4.1 The only safe way to exchange patient identifiable emails with external organisations is to send it from an nhs.net account and ensure that the recipient’s email address is also secure. The following table identifies Government systems allowing NHSmail users to share information confidentially and securely. Staff are responsible for ensuring that the email is being sent to a secure address. If in any doubt you should not send the information until you have confirmed that the recipient has a secure email address.

Sender	Recipient
xxx@nhs.net	xxx@cjsm.net (Criminal and Justice) xxx@gcsx.gov.uk (Local Government/Social Services) xxx@gse.gov.uk (Central Government) xxx@gsi.gov.uk (Central Government including Department of Health) xxx@gsx.gov.uk (Central Government) xxx@hscic.gov.uk (The Health and Social Care Information Centre) xxx@mod.uk (Military) xxx@nhs.net (NHSmail) xxx@pnn.police.uk (Police) xxx@scn.gov.uk (Criminal and Justice)

8.4.2 Staff should also ensure that the identity of the recipient to whom they are sending an email is correct, particularly where there may be more than one individual with the same name. If there is any doubt regarding their identity a non-confidential email should be sent to establish that they are the correct person before any confidential information is sent.

8.4.3 Owners of data are responsible for classifying their data and protecting it to the appropriate level of security/confidentiality before sending it by email. Under no circumstances is patient identifiable data to be sent to addresses other than those identified in Section 8.4.

8.4.4 If person-identifiable information is to be sent by email internally or externally via nhs.net, it should only be transferred in line with Caldicott Principles and the Data Protection Act. The Caldicott Principles govern the use of information about service users to ensure that the minimum amount of person-identifiable information is exchanged and only when absolutely necessary.

8.4.5 The Caldicott Principles:

- Justify the purpose(s) for using person-identifiable information.
- Only use person-identifiable information when absolutely necessary.
- Use the minimum amount of person-identifiable information that is required and only those items essential to the purpose.
- Access to person-identifiable information should be on a strict need to know basis.
- Everyone must understand and be aware of their responsibilities.

- Everyone should understand and comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality

Individuals have a right to see a copy of information held about them at any time under the Data Protection Act and this includes emails containing personal information.

8.5 Emailing patients/service users

8.5.1 It is recognised that email can be an efficient communication method between a clinician and service user. Email should only be used as a form of communication if it has been requested by the patient, in which case the clinician should initially ask the patient to email them thus providing a reply path containing the preferred email address. This will then reduce the risk of the wrong email address being used.

8.5.2 Inform patients about how emails are handled, including who will process email messages and who may contact them with a response. Safe Haven procedures must be used when sending confidential or sensitive information by email (see Safe Haven Policy).

8.5.3 It should be remembered that any correspondence with a patient will form part of the clinical record and as such will be governed by the usual storage and retention controls.

8.5.4 The form in **Appendix A** should be used when emailing patients. The risk associated with emailing patients includes, but is not limited to:

- The privacy and security of email communication cannot be guaranteed.
- Email to public internet email addresses (e.g. name@googlemail.com) is not secure at any point.
- An unlocked PC or publicly situated PC could result in a confidential email being left open to view.
- The email could be sent to the wrong patient, unless an email link is created.
- Emails can introduce viruses into a computer system, and potentially damage or disrupt the computer.
- Email addresses change, and patients should be reminded to inform you of any change of email address.

8.6 Personal use of email

8.6.1 Although LSW email system is meant for business use, the organisation allows the reasonable use of email for personal use and the following guidelines should be adhered to:

- Personal use of email should not interfere with work and should only be sent and read during breaks.
- Personal emails must also adhere to the guidelines set out in this Policy.
- Personal emails should be kept in a separate folder, named ‘Private’.
- No personal emails should be sent to ‘all staff’, or other groups of staff using LSW distribution lists.
- All messages sent including personal messages will remain the property of LSW.

8.7 Email system limitations

8.7.1 Staff using the email system will be bound by the following restrictions:

- The size of the mailbox will be limited to 200MB.
- The sending of attachments exceeding 20MB will be blocked.
- Emails in the Inbox which are marked as unread will be deleted after three months.
- Email accounts not accessed for three months will be suspended.
- Email will be subject to filtering using commercial software to enforce policy and reduce the impact of SPAM and/or malicious software.
- Where necessary email archive software is available.

9 Internet usage

9.1 Although LSW Internet is meant for business use, the organisation allows the reasonable use of Internet for personal use and the following guidelines should be adhered to (this would also be applied to portable devices).

9.2 Access to the Internet

9.2.1 Any person who wishes to access the Internet must apply to become an authorised network user. This is granted on request of the user and authorised by a sponsor using the Registration Authority (RA) process. For more information please contact the PICTS Service Desk on tel: 437000 (int. 37000).

9.2.2 If access is given to the Internet and is not used for at least a six month period, the account may be disabled. To re-enable the account the user must re-apply through the normal process.

9.3 Acceptable Internet use

9.3.1 Internet access is provided primarily for professional related purposes e.g. to access research material and other information relevant to your work. However, as access to many professional services are now provided over the Internet, LSW feels that reasonable personal use is permitted for authorised users on the basis that this does not interfere with normal work duties, the work of others or the network.

9.3.2 Personal Internet use must also adhere to the guidelines set out in this Policy.

9.3.3 Personal access to the Internet should be limited to outside of normal working times, and during designated breaks such as lunch time, unless authorised by the user's line manager.

9.3.4 PICTS are responsible for monitoring network usage, and if monitoring software identifies that there is excessive use of the Internet, the PICTS team will notify the Information Security Team who will raise the issue with the line manager of the individual.

9.3.5 As a guide a maximum of one hour would be deemed as acceptable personal use, although users should adhere to their manager's local guidance/instruction regarding personal use of the Internet.

9.3.6 Your line manager in conjunction with the Information Security Team, and Workforce Development will have the final decision of what constitutes excessive use.

9.3.7 Access to certain sites such as Facebook, Twitter and YouTube are permitted. However there are a number of websites which are blocked based on the following; their inappropriateness in the workplace, references to illegal or questionable activity, seen as a security risk to LSW infrastructure, or conflict with LSW's core values.

9.3.8 A list of the blocked sites can be obtained from the Information Governance team. Requests for exemptions can be made if a site is deemed necessary for a particular business or clinical function. These should be made directly to the Director of Professional Practice (Senior Information Risk Officer).

9.3.9 Staff who have innocently accessed an inappropriate site that has not been blocked or filtered will log off immediately and report this to their line manager and the Information Security Team by email to informationgovernancepht@nhs.net. Failure to do so may be subject to LSW's Disciplinary Policy.

9.4 Unacceptable Internet use

9.4.1 Creating, downloading, transmitting or displaying (other than for properly authorised and lawful research) any obscene or indecent images, any defamatory, sexist, racist, offensive, unlawful images, material that is designed to annoy, harass, bully, inconvenience or cause needless anxiety to other people (examples of offensive material are contained in the Dignity at Work Policy).

9.4.2 Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other user's data or hardware. It is a breach of security to download files which disable the network or which have the purpose of compromising the integrity and security of the network and file servers. You could be prosecuted the Computer Misuse Act 1990 and you will be subject to LSW's Disciplinary Policy.

9.4.3 Downloading/uploading executable files (a computer file containing step-by-step instructions in a form that the computer can follow) without the permission of the Information Security Team. These file types include, .exe, .com, .jap, .bas, .scr, etc. All file downloads must be virus-checked, and if you are unsure you should seek advice from the Information Security Team.

9.4.4 Using internet radio or streaming media, e.g. live video, without the permission of the Information Security Team, as this has a serious impact on the bandwidth available to network users and has an impact on clinical applications.

9.4.5 Using a proxy website to try and hide your identity from monitoring.

9.4.6 Having a device connected to both the corporate network and a public or third party network (e.g. via broadband modem) simultaneously, as this could introduce viruses or provide a route for unauthorised access.

9.4.7 Creating or transmitting "junk-mail" or "spam".

9.4.8 File downloads must be done in accordance with the Copyright, Designs and Patents Act.

9.4.9 Undertaking the activity outlined in points 9.4.1 to 9.4.7 will be subject to LSW's Disciplinary Policy, access to the individual's NT account being suspended pending investigation, access to place of work being removed, and/or prosecution. Other than instances which require criminal prosecutions, the final authority on what is or is not offensive material, or what is or is not permitted access to the Internet will be decided by the line manager in conjunction with Information Security and Workforce Development.

9.5 Use of social media and social networking sites

9.5.1 There are a vast number of social networking sites for both socialising and professional discussion. Staff have a personal responsibility both in and out of the workplace whilst using social networking sites to maintain patient and staff confidentiality and professional standards at all times. Unauthorised disclosure of business information could potentially be a confidentiality breach and subject to LSW's Disciplinary Policy.

9.5.2 Staff should keep information confidential about patients, staff, LSW, not engage in activities on the Internet which might bring LSW into disrepute e.g. inappropriate photographs, comments or descriptions of your personal activities etc., not post information when they have been asked not to, and remove information about a colleague if that colleague has asked them to do so.

9.5.3 If staff join a chat group or news group, they are expected to conduct themselves in an honest and professional manner. Staff are responsible for what they write and must be courteous and inoffensive. Unless staff are currently authorised to do so, they are not permitted to write or present views on behalf of LSW. This means that they cannot join a chat group in the name of LSW, or an NHS establishment or department, nor can they design a private website from their home PC and publish it under the name of LSW or an NHS establishment or department.

10 Fax usage

10.1 Person identifiable information which is to be faxed must be subject to Safe Haven procedures (see Safe Haven Policy). Safe Haven is a Caldicott term used in the NHS and Social Care Services for a set of procedures which explain to staff how to maintain the confidentiality of a person's information when it needs to be shared with other teams or organisations.

10.2 Guidance when using fax machines

10.2.1 In some limited circumstances it is acceptable to use fax machines to transfer person identifiable details and the following guidelines should be adhered to.

- The information transferred should be restricted to the minimum necessary and only those items of information that are essential to the purpose should be included.
- Care must be taken because fax machines often produce output of low quality, and even a missed decimal point could have disastrous consequences if the data were relied upon for patient care.
- In line with the Caldicott requirements information must be anonymised where possible by using for example the NHS number, or a hospital number.
- Names should only be used when absolutely necessary e.g. in those circumstances where there are no other common items between the parties.
- Care must be taken to ensure that errors are not made and information is not unlawfully disclosed to inappropriate locations.
- Where advice is needed, the Caldicott Guardian should be your point of contact.
- Fax machines should be sited in a secure environment where unauthorised staff cannot access them or view the information, and any faxes received out of hours are secure.

10.3 Examples of circumstances when a fax could be used to transmit person identifiable data are listed below.

- If other methods are not sufficient or other alternatives such as letter or encrypted electronic mail are not available.
- In an emergency, where delay would cause harm or the potential risk to the data

subject is greater than the risk of disclosure.

- When a letter of complaint arrives at an office other than the Customer Services Department, where compliance with National requirements (in this case, the time limit for acknowledgement of a response) is essential.

10.4 Agreed concessions where fax may be permitted

- Cancer care urgent referrals.
- Cases where alternative methods would not meet with the 0900 deadline for Out of Hours reports to be received at GP practices or relevant centres.
- Inter-practice and primary care to secondary care urgent referrals.
- The provision of urgent information to a GP from a secondary care provider.
- The timely management of patient transport involving West Country Ambulance Services NHS Trust.
- Transfer of urgent information between Health and Social Care Services.
- Urgent cases involving Community Mental Health Teams, Emergency Psychiatric Service and Out of Hours teams.
- Ordering of medication from pharmacy when there would otherwise be an unacceptable delay to treatment or discharge (refer to the Safe and Secure Handling of Medicines Policy and Procedure).
- Referrals - internal and external to the organisation.

10.5 Information which should not be faxed

10.5.1 The fax machine should not, routinely, be used for transferring sensitive information such as that concerning HIV status or drug misuse. Information such as incriminating evidence should never be submitted using facsimile equipment. No third-party information should ever be identifiable.

10.5.2 Where advice is needed, the Caldicott Guardian should be your point of contact.

10.6 Transmission procedure

10.6.1 Where patient information is to be transferred by fax, the following procedure should be followed wherever possible.

- Use a fax cover sheet that contains a confidentiality statement and clearly states who the fax is for (see Appendix B).
- Unless you are sending details to an unstaffed fax machine, for example out of hour’s reports, contact the recipient of the fax (or their representative) to let them know you are going to send confidential information.
- Ask the recipient to confirm receipt of the fax within an agreed timescale.
- Programme numbers into the fax machine memory where ever possible to avoid misdialling, otherwise confirm the number before the fax is sent.
- On completion retain the printed record of transmission as confirmation the fax was successful and include it with a copy of the cover sheet as proof of sending.

- If you are the recipient of a confidential fax you should ensure that you or someone on your behalf is at the receiving end waiting for it.
- No printouts should be left unattended at the fax machine.

10.6.2 Staff should report any actual or suspected breaches of security or potential weaknesses in the secure operation of the fax equipment to LSW's Security Officer, or Information Governance Lead who will investigate and record the incident in accordance with the Incident Reporting and Investigation Policy.

10.7 Logging of confidential faxes

10.7.1 If appropriate a logging system of confidential faxes sent should be set up and maintained. The log should include the following details as a minimum:

- Date and time.
- Sender's name and contact details.
- Recipient's name, phone number and organisation (as detailed on the cover sheet).
- A record of transmission from the fax machine on completion could also be held.

11 Mobile computing devices

11.1 This applies to all staff using LSW portable and remote working devices including but not limited to: laptops, palm tops (Personal Digital Assistants), remote working tokens, mobile phones and USB devices.

11.2 As the use of mobile technology and computing devices is growing it is vital that the data held on them is not compromised by poor security practices. Mobile technology and devices are by their nature vulnerable to both being mislaid as well as being attractive to a potential criminal. It is important therefore that all users of notebooks or laptops, Personal Digital Assistants (PDAs) and mobile phones are aware of the risks associated with their use, particularly away from the work place.

11.3 All NHS data on portable and remote working devices should only be saved on a trusted device that is encrypted to NHS standards.

11.4 Each staff member should be aware that there is an expectation to maintain an appropriate level of Information Governance as part of their contract of employment. This means that all personal information must be treated carefully and must not be disclosed to unauthorised persons.

11.5 Storing patient information on mobile devices

11.5.1 Mobile devices are not the safest means of storing patient information and care must therefore be taken to ensure we do not breach our personal and organisational responsibilities and ensure that patient confidentiality is not compromised.

11.5.2 Although we do not encourage patient information to be stored on mobile devices, there are certain exceptions as long as the following precautions are taken:

- No NHS Person Identifiable Data is to be stored on any portable machine or device (including a desktop PC) that is not encrypted.
- No NHS Person Identifiable Data is to be saved on a non-NHS device. The term non-NHS refers to equipment belonging to local authorities, social care, academic institutions and charities, as well as personally owned machines.
- NHS Data should only be saved on the LSW IT network, LSWs encrypted laptops or NHS standard self-encrypting USB Data sticks.
- All laptops, mobile phones and PDAs have a password functionality which enables users to password protect their devices. Staff must ensure they activate the password functionality to ensure their devices are password protected.

11.6 Repairs

- Portable devices that need to be repaired should be logged with the IT helpdesk. A replacement may be issued to the member of staff whilst the repairs are being carried out.

- It should be noted that manufacturers' warranties do not normally cover damage caused by misuse or neglect.

11.7 Permitted use

- Where a portable device is provided by LSW the portable device will be pre-loaded with software approved by the IT Department. Staff shall not load other software onto the device, upgrade software or in any way alter software without the express written permission of the ICT Services Manager.

- Staff must not make any hardware alterations or additions without approval from the PICT Services Manager.

- LSW reserves the right to audit correct usage at any time, and the individual may be held liable for illegally held software or material (e.g. in breach of copyright legislation).

11.8 Leavers

- Staff leaving LSW must return all their portable device(s) to their line manager. Line managers are be responsible for making sure that this is done and for returning equipment to the IT Department before it is re-assigned.

11.9 Internet connectivity and use

- Any portable device owned by LSW which has internet connectivity must be used in accordance with this policy and the Information Security Policy. Particular attention should be paid to the provisions relating to access to unsuitable material and activities which may compromise network security.

11.10 Wireless and other cordless connectivity

- Technological developments in the area of cordless connectivity (e.g. wireless connectivity, Bluetooth and infrared) have significantly increased the risks of unauthorised interception of a signal and of unauthenticated links being made to other devices. Staff should ensure these communication modes are switched off when not in use.

11.11 Digital imaging and videoing

- Photographs of service users are increasingly required for clinical or non-clinical reasons. Photographic recording techniques include photographic film, digital images and video. Any photographs or images are included within the scope of the Data Protection Act and attract the same levels of security and confidentiality.

- More information around digital imaging and videoing can be found in the Audio-visual Recordings of Patients/Visitors/Staff Policy the Department of Health's website: www.doh.gov.uk .

11.12 Working from home

- Within the workplace a number of security measures are taken to protect LSW property. Many of these are legal requirements of legislation such as the Data Protection Act 1998.

- It would clearly be unacceptable to allow staff who wish to carry on working on LSW information within the home to simply email, or remove on disk, documents to their personal PC systems. At the same time it is recognised that some staff may have a legitimate need to work on information at home and this policy sets out the ways in which that can be achieved with the primary aim of ensuring the security of the LSW information and compliance with legislation.

- LSW is not registered under the Data Protection Act for work carried out on computer equipment owned by a member a staff. Consequently, no LSW data of any kind should be accessed on privately owned equipment.

- No LSW or NHS data should be saved on to any non-LSW or NHS machine or device.

If a member of staff is working at home special safeguards are required:

- Workstations/devices provided by LSW used at home should be used exclusively for LSW business only and must be encrypted.
- Personal and sensitive information must not be stored on your personal computer/computing devices at home.
- Staff must have agreement from line management and must comply with all LSW and NHS standards and policies.
- Extreme care must be taken to ensure compliance with all relevant legislation, this may include software licence and copyright protection.
- Person Identifiable Data must only be stored on the LSW network or self-encrypting USB sticks.
- Great care should be taken with version control of data when operating from home to ensure that changes made are reflected in all stored versions.

When a workstation is connected between a home and LSW environment, adherence is required to the controls specified above.

11.13 Staff owned equipment

- The saving, copying and storage of person identifiable or confidential data on staff owned equipment is strictly forbidden. Staff may only use LSW supplied and encrypted machines and USB data sticks to store NHS data.

- For prevention of viruses and related security risks staff must not connect any personally owned devices to the LSW network.

- If files from your personal home computer are transferred to the office environment this should be done by using email for non-confidential data.

- Personal PDAs must not be connected to LSW-owned equipment and therefore cannot be used for work purposes. Staff requiring a PDA should contact the IT department who will advise on how PDAs can be used in a way that complies with LSW Policy.

11.14 Access control from remote locations

- LSW systems often need to be accessed from remote locations. This gives rise to extra threats, and in particular, the threat of unauthorised use and unauthorised access to systems and data.

- For the purpose of this Policy, ‘teleworking’ is defined as a member of staff whose ‘other’ authorised space to work is their home.

- The decision as to whether a member of staff will become a ‘teleworker’ will be made by their Executive Director, based on the frequency of work being done from home and the equipment required to support it.

- For the purposes of teleworking, LSW, at its discretion will provide such staff with a portable laptop. The laptop will remain the property of LSW and must be encrypted to NHS standards by the IT Department.

- All home computer connections for teleworking must be performed by the IT Department.

- Any ‘Remote worker’ will apply all elements of this Policy, but in addition will ensure:

    - Sensitive information (person identifiable or organisationally sensitive) is locked away when not in use and only accessible by the member of staff.
    - Any controlled document (e.g. patient record) they have will be traceable to their location and that any procedure to note the location of a file required by the organisation will be rigidly applied by them.
    - Their house and content insurance covers them for the loss of any equipment provided by the employing organisation.

12 Training

12.1 The LSW Information Governance Group has identified training needs for staff regarding this Policy. Training will be delivered at Corporate Induction and form part of the annual mandatory update for staff. Raising awareness will be managed through regular articles in LSW newsletter, the intranet and staff briefings.

13 Monitoring compliance and effectiveness

13.1 Monitoring compliance of this policy will be undertaken by LSW’s Information Governance Group and PICTS. Breaches of this policy are to be recorded as incidents using LSW’s incident reporting process. PICTS are responsible for the enforcement and monitoring of any access to the LSW network to establish breaches of the IT Security Policy. This encompasses all network access and includes internet access and email usage. PICTS are also responsible for ensuring for that suitable audit tools are in use which enforces policy. This information must be made available to NHS Security Managers of Connecting for Health and/or the NHS Counter Fraud Team on request.

All policies are required to be electronically signed by the Lead Director. Proof of the electronic signature is stored in the policies database.

The Lead Director approves this document and any attached appendices. For operational policies this will be the Locality Manager.

The Executive signature is subject to the understanding that the policy owner has followed the organisation process for policy Ratification.

Signed: Director of Professional Practice, Quality and Safety.

Date: 10th May 2016

Appendix A: Request for Livewell Southwest (LSW) to contact a patient via a personal email address

LSW is committed to open working and efficiency in providing services. To ensure that services are as tailor made as possible to the requirements of its patients LSW recognises that with advancing technology, current and routine forms of communication may not be convenient or possible with some patients. To this end LSW will be willing to undertake email correspondence with the patient under the following conditions.

- This agreement is entered into at the request of the patient.
- The patient understands that LSW has no responsibility for information that leaves authorised NHS (National Health Service) networks at the request of the patient and as such cannot guarantee the security of such information.
- The patient understands that LSW has no responsibility for equipment used by the patient to send or receive email.
- The patient has satisfied themselves that access to their own system is secure and are aware of shared email accounts, shared computers etc.
- To minimise the risk of 'human error' in writing email addresses, the patient will send an email to: _*insert clinicians email address here*_ in the first instance. This will give LSW their preferred email contact address and will be used to correspond with them. A test email will be returned by LSW to indicate safe receipt and that the sent address will be the one used to correspond with the patient.
- LSW reserves the right to terminate this agreement if there is any virus or other such technical threats to its internal systems as a result of external email traffic.

By signing below the patient indicates they have read and understood the conditions given above. The patient also understands they are able to review or cancel this arrangement at any time in writing.

Name: ____

Address: ____

Signature: ____

Agreed on behalf of Livewell Southwest

Signature: ____

Date: ____

Appendix B: Example fax cover sheet

Confidential Urgent Fax
Facsimile Transmission Cover Sheet

Livewell Southwest
Mount Gould Local Care Centre
200 Mount Gould Road
PL4 7PY

T. 01752 XXXXXX
F. 01752 XXXXXX
E. enquiries@....
www.webaddress.co.uk

From:			
Tel:		**Date:**	
Fax:		**Time:**	

To:	
Tel:	
Fax:	

Number of pages including cover sheet:
If you do not receive all of this fax please telephone 01752 XXXXXX

PRIVACY AND CONFIDENTIALTIY NOTICE

This communication may contain information that is strictly confidential. It is for the exclusive use of the addressee. If you are not the addressee, please note that any distribution, dissemination, copying or use of this communication or the information in it is prohibited. If you have received this communication in error, please telephone 01752 XXXXXX to arrange for its return.

Appendix C: Quick reference guide

Phones Introduction

- Private calls are those which are made for personal reasons, and not connected to LSW business.
- Private calls will be paid for by the staff member and requires line management approval.
- No reverse calls are accepted unless prior authority by the PICTS manager.
- Staff are unable to claim for home telephone line rental reimbursement.

Mobile Phones

- "Fair use" policy is implemented in respect of personal calls/text messages from LSW mobiles.
- If staff need to use their mobile for personal use a request must be submitted to the ICT Telecoms Team. A monthly salary deduction of £10 will be charged. Staff are expected to monitor their own personal usage to ensure it does not exceed £10.
- Personal abuse of LSW mobile phone is deemed as fraud and constitutes a disciplinary offence.
- Calls will be monitored.
- International calls from mobile phones are barred.
- On call staff have access to one mobile phone per rota.
- On call staff using a LSW mobile phone cannot claim reimbursement of home telephone line rental calls.

Use of Mobile Phones

- Only used in **non-clinical areas**.
- LSW staff should not receive private calls which affect the operational service of the department.
- Mobile phones to be switched off in clinical and ward areas.
- Silent ring tone to be used to avoid disturbing others.
- Mobile phones not to be used near electronic medical equipment.
- Mobile phone cameras not to be used.
- Mobile phones **must not** be used whilst driving.
- Evidence on use of SMS are within the full policy.

Email

- Do not use libellous, discriminatory, defamatory, offensive, racist or obscene remarks.
- Understanding copyright, trade-mark, libel, slander and public speech control laws.
- Do not forge email messages.
- Do not send emails from **another** person's email account.

- If the email is part of a clinical/corporate record this should be filed with the relevant record.
- Do not forward chain emails.
- Ensure antiviral precautions on the device are up to date.
- Ensure email address you are sending to is correct, there might be one individual with the same name – check as this is your responsibility and double check before sending confidential information.
- Use of illegal activity is grounds for immediate dismissal.
- User has the responsibilities of understanding copyright, trade-mark, libel, slander and public speech control laws.
- Emails are for LSW business but may be used for reasonable private use.
- Staff to use safe email addresses when exchanging confidential information.

Internet

- Internet access is primary for professional related purposes.
- Reasonable personal use is permitted as long as it does not interfere with the performance of duties.
- Personal use of internet is limited to outside of normal working times.
- Access to certain sites e.g. Facebook, Twitter and YouTube are permitted.
- Staff are not permitted to access sites such as pornography, gambling etc. or download offensive material.
- Staff are not permitted to interact radio or streaming media without permission from the Information Security Team.
- It is not permitted to download/upload executable files.
- Staff to maintain patient and staff confidentiality and professional standards when using social networking sites.

Fax machines and usage

- Staff to adhere to Safe Haven Policy.
- Faxes are permitted for:
  - There is no other method of sending the information.
  - In an emergency when a delay would cause harm.
  - Letter of complaint arrives at the wrong office and needs forwarding to Customer Services.
- Staff should not fax:
  - Routine transferring sensitive information concerning HIV status or drug misuse.
  - No third party information should be identifiable.
- Procedure:
  - Use fax cover sheet.
  - Telephone recipient prior to faxing.
  - Recipient to confirm receipt of fax.
  - Keep the printed transmission as confirmation of fax.
  - No printouts should be left unattended.

Glossary

Bandwidth

Bandwidth refers to how much data you can send through a network or modem connection. It is usually measured in bits per second, or "bps."

Blogging or Tweeting (micro-blogging)

Involves using a public website to write an on-line diary (known as a blog) or sharing thoughts and opinions on various subjects. Blogs and Tweets are usually maintained by an individual with regular entries of commentary, descriptions of events, and may include other material such as graphics or video.

Copyright

Copyright is a term used to describe the rights under law that people have to protect original work they have created. The original work can be a computer program, document, graphic, film or sound recording, for example. Copyright protects the work to ensure no one else can copy, alter or use the work without the express permission of the owner. Copyright is sometimes indicated in a piece of work by this symbol ©. However, it does not have to be displayed under British law. So a lack of the symbol does not indicate a lack of copyright.

Computer Misuse Act 1990

This Act makes it an offence to try and access any computer system for which authorisation has not been given.

Copyright Design and Patents Act 1988

Under this Act it is an offence to copy software without the permission of the owner of the copyright.

Data Protection Act 1998

This Act of Parliament governs the principles and arrangements required for the maintenance and appropriate disclosure of personal information.

Download/Upload

This is the process in which data is sent to your computer. Whenever you receive information from the internet, you are downloading it to your computer. For example, you might download brochure from a website. The opposite of this process – sending information to another computer is called uploading.

Executable Files

Many computer files are executable programmes, i.e. they actually do something, and they contain computer codes which might simply change the colour of your screen or might allow you to enter data into a form. Common executable files can be identified by their file ending, such as BAS, EXE, COM, JS, ASP etc.

N3
This is the name of the network supplied to the NHS and our entire internet and remote clinical systems use this network to transfer information.

Office of Communications (OFCOM)
The independent regulator and competition authority for the UK communications industries.

Safe Haven
Safe Haven is a term used to explain an agreed set of arrangements that are in place in an organisation to ensure confidential person identifiable information (e.g. patients and staff information) can be communicated safely and securely.

Security Incident
A security incident is defined as any event which has resulted, or could have resulted in for example; the disclosure of confidential information to any unauthorised individual, the integrity of the system or data being put at risk or the availability of the system of information being put at risk.

Social Media
Term commonly used for web-based and other mobile communications technologies that enable messages and opinions to be shared in dialogue with others who often share the same community interests. Such technologies can include blackberry messaging, instant messaging and other similar services.

Social Networking
The use of interactive web based sites or social media sites, allowing individuals on-line interactions that mimic some of the interactions between people with similar interests that occur in life. Popular examples include Facebook, Bebo, Myspace and Linkedin.

Teleworking
Teleworking is defined as a member of staff whose ‘other’ authorised space to work is their home.

USB
Universal Serial Bus.

Virus
Computer viruses are small programmes or scripts that can negatively affect the health of your computer. These malicious little programmes can create files, move files, erase files, consume your computer’s memory and cause your computer not to function correctly. Opening an infected email attachment is the most common why to get a virus.

For more information visit: http://www.sharpened.net/glossary/main.php