HPFT

Email, Internet & Intranet Policy

This policy gives guidance to staff on the Trust's use of Email, Intranet and Internet.

HPFT Email, Internet & Intranet Policy

Version	7.1
Executive Lead	Executive Director – Innovation and Transformation
Lead Author	Head of Information Rights and Compliance
Approved Date	9th March 2017
Approved By	Information Management & Technology/Information Governance Group
Ratified Date	9th March 2017
Ratified By	Information Management & Technology/Information Governance Group
Issue Date	31st May 2018
Expiry Date	9th March 2020
Target Audience	All staff who have access to Email, The Internet and The Trust Intranet

Document on a Page			
Title of document	Email, Internet & Intranet Policy		
Document Type	Policy		
Ratifying Committee	IM&T Senior Managers Meeting		
Version	**Approval Date**	**Review Date**	**Lead Author**
7.1	9th March 2017	9th March 2020	Head of Information Rights and Compliance
Staff need to know about this policy because -	Application of this policy will assist in compliance with the relevant Trust policies, information related legislation and NHS Standards and will ensure that all staff are aware of their individual responsibilities in regard to electronic communications.		
Staff are encouraged to read the whole policy but I (the Author) have chosen three key messages from the document to share:	• Individual responsibilities for all staff are outlined throughout the policy; • Clear guidance is given on the use of Email which is the main form of electronic communication used by the Trust; • The guidance given is essential in ensuring the transfer of data via electronic communications is as secure as possible.		
Summary of significant changes from previous version are:	The inclusion of Ransomware and Cybersecurity and overall annual policy review. Policy completed on new template. Updated list of automatically encrypted emails from the corporate and NHSMail accounts.		

Contents Page

PART 1 – Preliminary Issues

From 25th May 2018, the EU General Data Protection Regulations (GDPR) comes into effect. This is being incorporated within domestic legislation, which will become the new Data Protection Act (DPA). Until the new Act receives Royal Assent, this policy will continue to refer to either the GDPR or the more generic term of 'Data Protection Legislation'. For further information, please see the Trust's Information Governance Policy

1. Introduction

The Trust is an organisation committed to ensuring that diversity, equality and human rights are valued. We will not discriminate either directly or indirectly and will not tolerate harassment or victimisation in relation to gender, marital status (including civil partnership), gender reassignment, disability, race, age, sexual orientation, religion or belief, trade union membership, status as a fixed-term or part-time worker, socio-economic status and pregnancy or maternity.

The Trust works to a framework for handling personal information in a confidential and secure manner to meet ethical and quality standards. This enables National Health Service organisations in England and individuals working within them to ensure personal information is dealt with legally, securely, effectively and efficiently to deliver the best possible care to patients and clients.

The Trust via the Information Governance Toolkit provides the means by which the NHS and Partners can assess our compliance with current legislation, Government and National guidance.

Information Governance covers:

- Data Protection and IT Security (including smart cards),
- Human Rights Act,
- Caldicott Principles,
- Common Law Duty of Confidentiality,
- Freedom of Information Regulations, and
- Information Quality Assurance.

2. Summary

The Email, Internet and Intranet Policy sets out the commitment of the Trust to preserve the confidentiality, integrity and availability of electronic communications and to ensure that such electronic communications are effectively and lawfully managed.

Application of the policy will assist in compliance with the Trust's Information Security Policy, information related legislation, NHS Information Security Standards and NHS Information Governance Standards.

The Trust also recognises the need to share information with other health organisations and agencies in a controlled manner consistent with the interests of the service user and in some circumstances, the public.

3. Objectives

The Email, Internet and Intranet policy sets out the commitment of the organisation to preserve the confidentiality, integrity and availability of electronic communications and to ensure such electronic communications are effectively and lawfully managed.

The Policy aims to ensure that:

- The Email, Internet and Intranet services used by the Trust are secure and are operated in accordance with NHS Guidance, to industry standards and current best practice.
- The information contained in or processed by these systems is kept secure.
- Confidentiality, integrity and availability are maintained at all times.
- Staff are aware of their individual responsibilities and adhere to the provisions of the policy.
- Procedures are in place to detect and resolve security breaches and to prevent a recurrence.

4. Scope

This policy applies to:

- All Email, Internet and Intranet services used by the Trust and the information communicated electronically, processed or stored using these services.
- All staff employed by the organisation, contractors, seconded staff from other organisations and any other persons used by the organisation or engaged on the organisation's business.
- Any other persons granted access to the Trust's Email, Internet and Intranet services.
- All locations from which the Trust's Email, Internet and Intranet services can be accessed.

4.1 Legal Framework

This policy is compliant with relevant legislation, Department of Health and NHS regulations and guidance and the policies and procedures of partner organisations; principally, see Supporting References section.

5. Definitions

Email

- A system for sending messages from one individual to another via telecommunications links between computers or terminals.

Internet

- Also known as the 'Net', the single worldwide computer network that interconnects other computer networks enabling data and other information to be exchanged.

Intranet
- A privately maintained computer network that only authorised persons can access. Many corporations and institutions communicate with their employees or members through the use of a private intranet.

Encrypted
- To put computer data into a coded form.

Junk Mail
- Untargeted mail advertising goods or services.

Viruses
- Computer viruses can cause extensive damage shutting down a system or network.

6. Duties and Responsibilities

- The Board has responsibility for the management of all electronic information held and accessed by the Trust. This is devolved through the management line to all staff.

- The Information Management & Technology (IM&T)/Information Governance (IG) Programme Group reports on all aspects of Governance in this area. The Quality and Risk Committee receives reports on request.

- The Executive Director of Innovation & Transformation is the Executive Lead for Information Governance within the Trust.

- The Associate Director of IM&T has operational responsibility for Information Governance within the Trust.

- Senior Information Risk Owner (SIRO) is an Executive who is familiar with and takes ownership of the Trust's information risk policy and acts as an advocate for information risk to the Board. They have lead responsibility to make sure the Trusts information risk is properly identified, managed and that appropriate assurance mechanisms exist.

Part 2 – What needs to be done and who by

7. Electronic Mail and Internet Services

Email, Internet and Intranet services are provided solely for the conduct of official Trust business and are subject to the Trust's Information Security Policy.

These services and the associated systems and information are the property of the Trust. This includes all hardware, software and all data that are stored within the systems, any messages, attachments, and downloads.

8. Permissible Uses of Electronic Mail and Internet

8.1 Authorised Users

Staff will be given a username and/or a smartcard and a password to access the systems they are authorised to use. These will identify the user to the system.

Contractors, temporary staff and other persons working on behalf of the Trust may be given authority to use these services in accordance with the Trust's policies and subject to appropriate authorisation.

8.2 Purpose and Use

The use of any Email, Internet and Intranet resources must be related to the legitimate business activity of the Trust and its partners. This includes authorised professional and academic pursuits.

Incidental and occasional personal use of Email, Internet and Intranet may be permitted at the discretion of the appropriate senior manager. Any personal use will also be subject to the provisions of this policy.

In all cases, staff are required to use their best judgement in using these systems to ensure they do not create, post or send information, images or files that would be likely to affect the reputation, security, efficiency or perception of the Trust. This extends to include uses that are intended to be private or personal.

All staff have a responsibility to ensure they don't breach any of the key Data Protection Principles. If this does occur, the Information Commissioners Office (ICO) may decide to take action against the Trust and in serious cases we could incur a fine of up to 4% annual global turnover or €20 million, whichever is greater.

8.3 Transmission of Confidential Information

All person identifiable data (PID) must be encrypted in accordance with DH standards, before or during transmission, and removed from the device (i.e. memory stick, external hard drive) when completed. All Trust Laptops, portable hand held devices e.g. Smart phones and memory sticks, must be encrypted and backed up on a regular basis. All devices must be used and stored securely. Refer to - Guidance on the use of Email when sending PID (Appendix 1) - for further information.

8.4 Prohibited Uses of Email and Internet

- Use of another person's identity (username/password or smartcard) to access Email, Internet and Intranet services;
- Use of Email, Internet and Intranet resources for personal monetary gain or for commercial purposes that are not directly related to the Trust's business;
- Personal use that creates a cost or inconvenience for the Trust;
- Intercepting or opening Email or electronic files addressed to another recipient without their permission (except for authorised employees in the course of The Trust's business);
- Use of Email to harass or intimidate others or to interfere with the ability of others to conduct the Trust's business;
- Disguising an Email identity in an attempt to deceive the recipient of the source or identity of the sender;
- Use of electronic mail systems for any purpose restricted or prohibited by law or regulations;
- Inclusion of the work of others into Email in violation of copyright laws. Employees have a responsibility to ensure that copyright and licensing laws are not breached when composing or forwarding Emails and Email attachments;
- Unauthorised access or attempted access to Email or attempted breach of any security measures on any systems;
- Viewing, distributing or contributing to illegal or inappropriate materials on the internet, including material that might be offensive to others;
- The distribution of chain letters, inappropriate humour, explicit language or offensive images or material;
- Downloading of any files that could jeopardise the security and integrity of the Trust's networks or systems;
- Injudicious use of work time and facilities for private purposes;
- Discussing sensitive or confidential work-related issues at any time online, e.g. on personal social network sites, including conversations about service users or complaints about colleagues. Even when anonymised, these are likely to be inappropriate. Please refer to the Trust's Social Media Policy for further guidance.
- The sending and receiving of NHS related information, especially PID using public Email systems (Gmail, Hotmail, Yahoo, Facebook, Twitter etc.) other than in compliance with this document.

8.5 Restrictions on Internet Sites

Restrictions will be placed on access to any internet site that could be regarded as a threat to services, systems and resources, that interferes with the use of the network or other services or to any site that is considered inappropriate.

This will include, (but is not limited to):

- Sites that attempt to propagate malicious code or any other threat;
- Sites containing information that is inappropriate, offensive or unlawful, (such as pornography, racial bias, social networking, gambling and games);

- Downloads or data transfers that threaten or interfere with network or other resources (such as executable files and media streaming);
- Sites that provide 'cloud-based' storage functionality (such as huddle, SkyDrive, iCloud, Dropbox, etc.) except where explicitly approved.

8.6 Use of Social Media

Please see the Trust's Social Media Policy.

8.7 Contents of Messages and Internet Material

Messages and Internet material must not contain anything that may be considered offensive or disruptive to the Trust or its stakeholders. Offensive content would include, but would not be limited to, sexual comments or images, illegal or unauthorised software, racially biased materials, gender-specific comments or any comments/material that would offend someone on the basis of his or her age, sexual orientation, religious or political beliefs, national origin, or disability. Messages and internet material must not contain anything which could be regarded as libellous.

8.8 Inappropriate or Offensive In-bound Email

Inbound Emails may contain inappropriate or offensive material that is beyond the control of the Trust. Receipts of such Emails should be reported to the ICT Department's Service Desk.

8.9 Unsolicited or 'Junk' Email

This is Email received from senders you do not know or companies you do not do business with. Examples are unsolicited advertising for goods or services or warnings of supposed new viruses. These Emails should be deleted without opening them. Do not forward or reply to such Emails, click on adverts or visit sites contained in such Emails.

8.10 Accidental Access to Inappropriate Material

If inappropriate material is accessed accidentally, users shall immediately report this to the IT service desk so that this can be monitored appropriately. Users should report any such incidents to an appropriate line manager.

8.11 Viruses, Ransomware and Cybersecurity

Ransomware originates from compromised websites, Email phishing and other malware. Deliberate introduction of any damaging malicious software is a crime under the Computer Misuse Act 1990. All of the organisation's computer equipment has malicious software checking installed. See Appendix 5 for further information and guidance.

It is the responsibility of individual users to ensure that all computer files are malicious free.

If material is inadvertently accessed which is believed to contain malicious software, the user should immediately break the connection, stop using the computer, and contact the service desk.

8.12 Privacy and Confidentiality

The nature and technology of electronic communication means that the privacy of an individual's use of the Email system, or the confidentiality of messages, cannot be ensured. Messages may be received or monitored by someone other than the intended recipient.

All reasonable efforts will be made to maintain the integrity and availability of Partnership's electronic communications systems. However, the Trust systems should not be relied upon as a secure medium for the communication of sensitive or confidential information. All staff MUST comply with the Trust's Guidance on the Use of Email (Appendix 1).

9 Access and Disclosure of Electronic Communications

9.1 General Provisions

To the extent permitted by law, the Trust reserves the right to access and disclose the contents of any electronic communications without the consent of the user. This right will be exercised when there is believed to be a legitimate business reason to do so including, but not limited to, those listed in ***Section 9.2*** and ***9.3*** below and with the authority of a Director of the Trust.

The Email systems should be treated like a shared filing system, i.e., with the expectation that communications sent or received may be made available for review by any authorised employee for purposes related to the Trust's business.

Email may constitute 'personal records' and be subject to the provisions of Data Protection Legislation and the Access to Health Records Act 1990. The data subject has the right to access any such records.

9.2 Monitoring Communications

To the extent permitted by law, all electronic communications and their content will be monitored for purposes of:

- Maintaining the integrity and effective operation of systems managed or supported by the Trust.
- Ensuring compliance with the Trust policies and procedures and compliance with legislation and statute law.

The Trust retains the right to access, review, copy, and delete any material created, stored or transported on its systems. This includes but is not limited to messages sent, received or stored on the Email system and any material accessed or downloaded from the internet.

Volumes of electronic communication will be monitored routinely including the source, destination and subject of the communication.

9.3 Inspection and Disclosure of Communications

The Trust reserves the right to inspect and disclose the contents of electronic communications:

- To discharge legal obligations and legal processes and any other obligations to employees, clients, patients, customers and any third parties (in particular, when disclosure is requested under provisions of Data Protection Legislation or the Freedom of Information Act 2000).
- To locate substantive information required for Trust business that is not readily available by other means.
- To safeguard assets and to ensure they are used in an appropriate manner.
- In the course of an investigation into alleged misconduct.

9.4 Special Procedures for Monitoring and Disclosure

Prior approval must be obtained from the appropriate Director to gain access to the contents of electronic communications or data stores, and disclose information gained from such access.

10 Disciplinary Action

Breach of any aspect of this policy will be subject to disciplinary action in line with the Trust's disciplinary policies. Serious breaches will be regarded as gross misconduct and may result in dismissal.

11 Training

There is no formal training, this is monitored via supervision; all staff should review annual Information Governance Training.

Course	For	Renewal Period	Delivery Mode
Information Governance/Data Security Awareness	All Staff	Annually	E-Learning Classroom

12 Embedding A Culture of Equality & RESPECT

The Trust promotes fairness and RESPECT in relation to the treatment, care & support of service users, carers and staff.

RESPECT means ensuring that the particular needs of 'protected groups' are upheld at all times and individually assessed on entry to the service. This includes the needs of people based on their age, disability, ethnicity, gender, gender reassignment status, relationship status, religion or belief, sexual orientation and in some instances, pregnancy and maternity.

Working in this way builds a culture where service users can flourish and be fully involved in their care and where staff and carers receive appropriate support. Where discrimination, inappropriate behaviour or some other barrier occurs, the Trust expects the full cooperation of staff in addressing and recording these issues through appropriate Trust processes.

13 Process For Monitoring Compliance With This Document

The strategy will be reviewed annually. The Information Rights and Compliance Team will have a key role in monitoring progress and will report regularly to the Trust Audit Committee.
Progress will be monitored by:

- The results of audit programmes
- Compliance with NHS Information Governance criteria
- Information Governance Toolkit
- Compliance with this policy will be monitored both electronically and by means of audits and spot checks.

Action:	Lead	Method	Frequency	Report to:
Check policy for compliance with the Information Governance Toolkit	Senior Information Governance Officer	Annual Review	Yearly	IM&T/IG Programme Group

13.1 Promoting and Considering Individual Wellbeing

Under the Care Act 2014, Section 1, the Trust has a duty to promote wellbeing when carrying out any of their care and support functions in respect of a person. Wellbeing is a broad concept and is described as relating to the following areas in particular:

- Personal dignity (including treatment of the individual with respect);
- Physical and mental health and emotional wellbeing;
- Protection from abuse and neglect;

- Control by the individual over day to day life including over the care and support provided and the way in which it is provided;
- Participation in work, training, education, or recreation;
- Social and economic wellbeing;
- Domestic, family and personal;
- Suitability of living accommodation;
- The individual's contribution to society.

There is no hierarchy and all should be considered of equal importance when considering an individual's wellbeing. How an individual's wellbeing is considered will depend on their individual circumstances including their needs, goals, wishes and personal choices and how these impact on their wellbeing.
In addition to the general principle of promoting wellbeing there are a number of other key principles and standards which the Trust must have regard to when carrying out activities or functions:

- The importance of beginning with the assumption that the individual is best placed to judge their wellbeing;
- The individual's views, wishes, feelings and beliefs;
- The importance of preventing or delaying the development of needs for care and support and the importance of reducing needs that already exist;
- The need to ensure that decisions are made having regard to all the individual's circumstances;
- The importance of the individual participating as fully as possible;
- The importance of achieving a balance between the individuals wellbeing and that of any carers or relatives who are involved with the individual;
- The need to protect people from abuse or neglect;
- The need to ensure that any restriction on the individual's rights or freedom of action that is involved in the exercise of the function is kept to the minimum necessary.

Part 3 – Document Control & Standards Information

14 Version Control

Version	Date of Issue	Author	Status	Comment
Draft V1	17/10/08			Initial draft based Trust's Information Security Policy & NHS Information Security Codes and Guidance of Practice,
Draft V1	10/02/09			Revised in line with changes in national guidance and practice, also amended to include reviewer comments.
Draft V2	15/05/09			Revised into Trust standard format.
V2	01/09/09	Information Governance Officer	Published	Agreed by EXEC
V3	11/10	Information Governance Officer	Draft	Annual Review
	01/11	Information Governance Officer	Draft	Ratified by IG&R Group via E Mail
	01/11	Information Governance Officer	Draft Final	Sent to Exec for final ratification Ratified by Exec 1st February 2011
V3.1	01/11	Information Governance Officer	Final	Addition of E Mail Guidance version V.1.1 as appendix, Agreed by IG&R Group 20/10/2011
V4	2/12	Information Governance Officer	Draft Final	Annual Review – Social Networking sentence added to 5.2 Link to NMC Website and Appendix B Appendix C - GSCC Professional Boundaries Guidance 2011 Approved by IG&R Feb 2012 and Via Email 8th March 2012
V5	22/13	Information Governance Officer	Final	Approved by IM&T 17th June 2013
V6	26/03/15	Head of Information	Current	Annual Review – Added instructions for sending

		Governance and Compliance		confidential emails in Outlook 2007/2010 and Service User Email guidance.
V6.1	30/09/15	Senior Information Governance Analyst	Final	Annual review – change to encryption method of email
V7	09/03/2017	Senior Information Governance Officer	Final	Annual Review – Addition of ransomware and cybersecurity
V7.1	31/05/2018	Senior Information Governance Officer	Final	Annual Review – updated list of automatically encrypted emails from the corporate and NHSMail accounts

15 Relevant Standards

- Information Governance Toolkit (IGT) V14.1 Requirement 308
- NHS Encryption Standards published in December 2008
- NHS Information Security Code of Practice 2007
- Equality and RESPECT: The Trust operates a policy of fairness and RESPECT in relation to the treatment and care of service users and carers; and support for staff

16 Associated Documents

- Confidentiality Agreement
- Data Quality Policy
- Social Media Policy
- Information Risk Policy
- Information Security Policy
- Information Governance Policy
- Learning from Incidents Policy
- Freedom of Information Act Policy and Procedures
- Protection & Use of Service User Information Policy
- Written & Electronic Communications Policy
- Data Protection Legislation
- The Freedom of Information Act 2000
- The Access to Records Act 1990
- Human Rights Act 1998 (Article 8)
- Computer Misuse Act 1990

17 Supporting References

Information Governance is the framework which brings together all of the requirements, standards and best practice that apply to the handling of electronic information. The areas that are included within Information Governance are:

- Data accreditation and data quality
- Caldicott sharing of patient identifiable information
- Consent to sharing of personal information
- ISO27001 – Information security management
- Common law duty of confidentiality
- Data Protection Legislation
- Records Management
- The Freedom of Information Act 2000
- Human Rights Act 1998 (Article 8)
- Professional Standards

NHS DIGITAL: Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.

NHS DIGITAL: Good Practice Guidelines in Information Governance – Information Security.

DH: NHS IG – Guidelines on Use of Encryption to Protect Person Identifiable and Sensitive Information 2008

DH: Information Security NHS Code of Practice 2007.

DH: NHS IG – Information Risk Management – Good Practice Guide 2009.

NHS IG – Detailed Guidance on Secure Transfers of Personal Data.
NHS DIGITAL: Sending an encrypted email from NHSmail to a non-secure email address.

18 Consultation

Approval and ratification process for this document by Information Governance and Records Group and HPFT Policy Panel.

List of people/groups involved in the consultation.

Risk Management	
Acute Service Manager	Caldicott Link
Community Service Manager	SIRO Link
LD & Forensic Service Manager	Consultant Psychiatrist, (Deputy Chair)
Information Security Manager	**Information Governance Officer**
HR Manager	Head of Information Rights & Compliance
Clinical Lead	
Social Care	

Part 4 Appendices

Appendix 1

Guidance on the use of Email when sending person identifiable or confidential information

Staff must establish whether the recipient of the Email can receive the information in a secure manner, patient information has to be encrypted.

Your @**NHS.net** address is secure when sending personal identifiable information to the following Email accounts**:**

- @hscic.gov.uk
- @x.gsi.gov.uk
- @gsi.gov.uk
- @gse.gov.uk
- @gsx.gov.uk
- @whht.nhs.uk
- @police.uk
- @pnn.police.uk
- @cjsm.net
- @scn.gov.uk
- @gcsx.gov.uk
- @mod.uk

Further guidance on encryption from @NHS.Net can be found at https://portal.nhs.net/Help/policyandguidance along with an up to date list of emails that are automatically secure in addition to the above.

Any email domain not listed above or included in the accredited list of domains in the above link, will need to be encrypted – guidance can be found here.

Please see dos and don’ts list below:

Dos and Don’ts

- When sending person identifiable data (PID) always ensure you have chosen the correct recipient
- You must follow the instructions below when sending PID to an email account not listed above
- You **can** send PID to nhs.net accounts from corporate email accounts (see description above).
- Emails containing PID should only be sent to those individuals who have a legitimate need to see the information
- **Do not** send PID to or from personal email accounts e.g. Hotmail, Google etc. unless the recipient is also the data subject or representative in this case you will need to encrypt the email as outlined in Appendix 1.
- Attachments containing PID sent to corporate accounts as listed above **do <u>not</u>** need to be password protected.
- Members of staff should always ensure that they send the minimum amount of PID. If it is not absolutely necessary it should not be shared, whatever the mechanism.
- The Caldicott principles[1] must be applied when sending emails containing PID.
- Do review the Trusts Email, Internet and Intranet Policy

[1] The Caldicott principles must be applied when sending emails containing PID, for example, only send the minimum amount of PID; such emails should only be addressed to individuals who have a right to see the information

Frequently Asked Questions

What is safe and secure email?
Securely sending and receiving email means that the contents and attachments of the email are secure whilst in transit to the recipient.
What is encryption?
Encryption is scrambling the email before sending and applying a secret password to unscramble. If you are using corporate email and sending it to other corporate email address as defined on page 19, encryption is set by default and is a seamless process. You do not need to set any passwords. It is important **not to** alter the security settings in Outlook. If you are emailing confidential emails outside the corporate email system there are additional steps to follow to encrypt the email. Separate instructions on how to do this are shown in Appendix 1.
When should email be encrypted?
Any email that is confidential must be encrypted.
Can I send or receive confidential email to staff using NHSMail (@nhs.net) from my corporate email account? (see page 19 for definition)
Yes, emails are now automatically encrypted.
Can I receive confidential emails if I am using corporate Email (see page 19 for definition)
Yes You are able to received confidential emails
Can I receive encrypted or password protected documents if I am using corporate email.
Yes
Can other organisations receive and send encrypted email
That very much depends on their internal email set-up. In most cases the answer isyes.
If a patient has emailed into the Trust from their home email address requesting confidential information about them can I respond?
Yes but you need to use the instructions on page 20**.**
I don't use corporate email (e.g. @hpft.nhs.uk), I use NHSMail (@nhs.net)
Users of NHSMail can send confidential email to corporate emails or to other users of NHSMail and to the governance emails listed above
Is my email confidential?
If the email contains corporate sensitive data, staff or patient/personal identifiable information, then it is confidential.

Appendix 2

Guidance on Protecting your Confidentiality when sending an Email to the Trust

- Email the minimum amount of personal information that is required in order for us to provide you with the appropriate service.

- If you decide to send sensitive details from your personal email account (Hotmail, Google etc.) including detailed information about your care and treatment, we would recommend the following:

    - Put your information in a Word document and password-protect it.

    - You will need to notify the intended recipient of the password so that they can open it up once they have received it.

    - Passwords should never be sent by email; contact the intended recipient by phone to let them know what your password is (Guidance for password protecting a word document is below) or

    - Use encryption software for your personal Emails details, free email encryption for Microsoft Outlook can be found at http://www.sendinc.com/software/outlook-email-encryption-add-in

- Check that you have the correct email address for your intended recipient before you press send.

As an extra precaution it is strongly recommended that you:

- Only use a home computer and not a public computer.

- Install a firewall, virus checker and anti-spyware software on your computer as a virus infected machine may maliciously resend your Emails to all your Email contacts.

Password Protect a Document

You can protect a document by using a password to help prevent unauthorized access. Please remember Microsoft cannot retrieve forgotten passwords

In Office 10:

1. Click the File tab.
2. Click Info.
3. Click Protect Document, and then click Encrypt with Password.
4. In the Encrypt Document box, type a password, and then click OK.
5. In the Confirm Password box, type the password again, and then click OK

For earlier versions of MS Office

1. Click Microsoft Office Button , point to Prepare and then click Encrypt Document.
2. In the Encrypt Document dialog box, in the Password box, type a password and then click OK.
3. In the Confirm Password dialog box, in the Re-enter password box, type the password again, and then click OK.

To save the password, save the file.

Appendix 3

What is RANSOMWARE?

Ransomware is malware used to “kidnap” a user’s information by encrypting it and demanding payment as a ransom for its release.

Once installed on the user’s computer, this “file coder” code will encrypt the user’s information and demand a payment as ransom in exchange for a password which will decrypt the information. If the user pays the ransom, the key will work only on their infected system and cannot be used to save another person’s infected computer.

It is usually installed on computers by clicking on shipping or banking email attachments (UPS, FedEx, ADP, and various large banks) that contain a virus. Even if you don’t have administrator rights on the computer, it will still install and attack.

What can I do to minimise the risk of this happening to me?

- **Avoid giving out your email address.** Attackers collect email address, which they find by searching on publicly accessible websites (such as web forums). They gather a large number of email accounts in order to propagate malicious code, or to carry out other malicious activities like sending spam, launching unsolicited advertising campaigns, or mounting phishing attacks.
- **Check the content of the messages you receive and send.** It’s essential to check the content of the messages we receive by email. Email attachments have become a very common method for spreading malware - one of the main means of infection by Ransomware. Checking sender’s messages, taking care with ‘too tempting’ to resist offers, checking it is really an email, and not clicking on suspicious links are basic measures to avoid falling victim to tricks that might result in infection. These should be combined with other good practices for looking after your email.
- It is also important to check information sent, recipients and attachments. Sensitive information could be sent by mistake to the wrong recipient or malware might be sent unwittingly.
- **Don’t click on any links or use the phone numbers in the email.** If you receive a suspicious email (phishing), but are not sure, contact the company by visiting their website or via phone.
- **Try not to click on ads for products or companies you don’t know.** If you see an appealing ad, go directly to the company’s website and see if the offer is there.

Awareness is key! As a computer user, your job is to stay aware of what’s happening on your device. You don’t have to be a computer security expert to practice safe clicking. Even the safest computer users can get infected with malware. By staying alert and aware you can dramatically reduce your chances.

If you suspect that you have been a victim of an attack and your computer has been infected with spyware due to suspicious activity please seek assistance from the IT Service Desk via email on servicedesk@hblict.nhs.uk or by calling 01707 685562.

Our Values

Welcoming Kind Positive Respectful Professional