User Information Security Policy

2016

User Information Security Policy

November 2016

Version 1.0

Frank Rankin

Information Governance Manager

NES Digital

frank.rankin@nes.scot.nhs.uk

Contents

Objective

The objective of this policy is:

- to provide NES users with the information required to understand their responsibilities and provide clear guidance on information security procedures
- to ensure the Confidentiality, Integrity and Availability of all NES information assets
- to protect NES information assets from threats, internal or external, deliberate or accidental

This policy sets out clear direction, support and responsibilities for users of NES information systems and assets, to meet business requirements, legislation, regulations, standards and guidance. [ISO/IEC27001:2013 5.2]

NES is committed to satisfying the requirements of ISO/IEC27001:2013 and all current NHSScotland information security policies and guidance in meeting its information security objectives [ISO/IEC27001:2013 5.2c]

Scope & Applicability

This policy applies to all users of NES corporate information systems and assets who undertake work for NES or use any part of the IT infrastructure, whether as an employee, a trainee, a student, a volunteer, a contractor, partner agency, external consultant or 3rd party IT supplier.

This policy refers to information in any format or medium held on NES premises, equipment and infrastructure, on cloud or other hosted environments, on NHSScotland national systems, or held by NES employees or third parties on behalf of NES. Attention is given to the interaction of users between information systems and NES assets and how this should take place.

For details of the legislative, regulatory and guidance framework within which NES manages our information governance and security, see the Corporate Information Security Policy.

Your responsibilities – All staff and contractors

(For details of specific corporate roles, see IGP04 Corporate Information Security Policy.)

All NES staff, contractors and service providers who use or influence the use of NES information systems must conform to the standards expected and described in this and any other associated information security policies.

All staff must read and, where required, sign up to any information security policies or procedures which are relevant to their job role and information tasks.

Specific information security responsibilities required of key personnel will be defined in their job description and within IT systems secure operating procedure documentation.

Secure workplace practices are an essential part of this Information Security Policy. NES expects all staff to take personal and professional responsibility for dealing securely with any information they have access to in the course of their duties.

Every member of staff is personally responsible for ensuring that no breaches of information security result from their personal actions. This is equally applicable for staff authorised to access and use NES Information systems remotely.

Staff must immediately report through NES Corporate Digital helpdesk (Service Now) and to their Line Manager any suspected or actual information security events or incidents. If they cannot immediately access the IT helpdesk they should email or telephone Corporate Digital Services. (ISO27001:2013 A 7.2.3)

Failure to observe this policy may result in disciplinary action under the NES disciplinary policy. (ISO27001:2013 A 7.2.3)

All users are required to exercise care in securing mobile devices for which they are responsible and which hold NES data or documents, and to report any loss or theft to Corporate Digital Services immediately to allow mitigating actions to be taken.

Summary - Key things to remember

Acceptable Use of NES Assets

- All users must keep passwords and authentication tokens secure
- NES systems and devices should be used for purposes related to your NES duties. They must never be used for commercial, political or campaigning purposes
- Moderate personal use of NES email, telephones and internet is permitted, but NES email is a corporate tool and personal private cannot be assured
- Non-NHS webmail must not be used for NES business purposes
- All NES data must be held on online or network storage, rather than laptop or PC hard-drives or removable media.

Clear desk and screen

- Desks must be kept clear of documents and files when not in use, and cleared and available for use by other colleagues on departure from the office
- Screens must be locked when not attended ⊞ + L

Mobile device and teleworking

- All NES-owned mobile data storing devices must be encrypted
- Personal mobile devices used for NES purposes must be identified to and managed by the Mobile Device Management system
- You must inform Corporate Digital Services immediately if a NES device is lost
- When remotely accessing NES systems, you must ensure that NES documents are not cached or stored on home or public PCs or other devices at the completion of work, for example when working on documents downloaded from Office 365

Incidents and risk

All NES staff must inform Corporate Digital Services and their line manager of any suspected or actual incidents affecting information security

Access to NES systems and data

Staff, contractors and others will be provided with role-appropriate access to NES systems and data. No attempt should be made to access systems or data which are not authorised.

Within the Office 365 SharePoint environment, an open access policy is in place whereby documents and information are visible to all NES users unless there is a business or compliance reason to restrict access. Users must not abuse this approach by inappropriately editing, downloading or further sharing information outwith their area of authority.

Access controls are typically secured through issue of a username and password. All users must protect passwords for NES systems from disclosure and must never share them with others, even within NES. Passwords should be deliberately obscure to and difficult to guess and must not be written down or otherwise recorded where they could be accessed by others. Usernames, NES email addresses and passwords used for NES systems must not be re-used on third party applications (such as non-NHS internet based tools) where they may be hacked and used to breach NES security. (ISO27001:2013 9.3.1)

Users are not permitted to download or install software on NES systems or devices. Users will not have administration rights on PCs or laptops unless specifically authorised by Corporate Digital Services to fulfil a specific technical role. (ISO27001:2013 12.6.2)

Acceptable use of NES assets and systems

(ISO27001:2013 8.1.3)

The NES systems and applications, NES Office 365 domain, telephones and access to the Internet from the NES network are provided as tools to assist NES employees in their work. Moderate personal use of email and internet is permissible provided this does not impact on productivity through distracting staff or placing inappropriate loads on systems, for example excessive use of internet bandwidth. Personal use should be limited and outwith core times. Office 365 is a corporate communications system and, while reasonable efforts would be taken to respect the privacy of personal communications, there can be no expectation of personal privacy for emails within the system.

No NES system or device may be used to send, store or forward offensive or inappropriate content. This includes:

- Indecent, offensive or illegal images or text;
- materials which breach copyright or Intellectual Property Rights;
- material which is libellous, defamatory, bullying, harassing or obscene;
- materials which otherwise pose a risk to NES systems or to the reputation of NES.

Receipt of such content should be reported to line management to identify whether further action is required under NES policies.

No NES system or device will be used to store or transmit patient or service user data, except for exceptions identified to Information Governance and approved by the Caldicott Guardian.

Audit and logging

Use of NES systems, including internet access and email, creates an audit trail which can identify activities of individual members of staff. Incoming and outgoing e-mail messages, the history of internet sites that employees have visited and text messages sent and received through NES devices are all accessible to and auditable by the organisation. Where it is necessary for business or audit purposes to access email or other communications in an employee's absence, NES will take reasonable steps to protect privacy, ensuring that as far as practical no unwarranted access to private emails is obtained and that confidentiality is maintained. However, NES can give no guarantee of privacy where staff choose to make personal use of NES systems.

NES will not monitor individual staff members' use of systems on an ongoing basis, but NES management may receive occasional reports showing patterns and levels of internet use.

Where there are significant concerns relating to inappropriate use of systems, and where formally authorised by the Workforce Directorate, audit evidence from systems may be used as part of the investigation of individual staff conduct.

Where evidence of criminal activity is discovered, NHSScotland Counter Fraud Service and the police may be informed and given access to NES audit logs and system content.

Physical assets – PCs, laptops, tablets, phones, flash drives

NES staff and contractors are issued with NES equipment to fulfil their contractual duties. Such equipment remains the property of NES, will be managed and tracked as an asset and must be returned to NES at the conclusion of employment or contract, or when requested by Corporate Digital Services. (ISO27001:2013 8.1.4)

Corporate Digital Services reserves the right to recall NES devices at any time. NES users should ensure all significant information and data are kept on online storage (such as SharePoint or OneDrive) to avoid reliance on device storage.

NES information assets (including ICT equipment, records, and data must not be removed from NES premises without prior authorisation (ISO27001:2013 11.2.5). Other than devices issued for the purposes of mobile working (laptops, tablets, phones, flash drives), any other removal of NES equipment must be approved and recorded by Corporate Digital Services. The asset must be returned to NES premises at the agreed time.

NES mobile devices must not be left unattended and users must take all appropriate measures to keep devices secure when travelling or working away from NES premises. (ISO27001:2013 A11.2.8, 11.2.6) When not using mobile devices, users must be logged out to ensure encryption is enabled. Any loss or suspected loss of a NES mobile device must be reported to NES Corporate Digital Services **immediately** to permit mitigation steps to be taken.

Recording of Meetings

The term ‘recording’ covers any type of audio and video recording device, including personally owned equipment. No recording of any meeting may be made without the express agreement of all participants at the meeting. Transcripts and a copy of the recording will be made available unless agreed otherwise.

Covert recording of a meeting would be illegal under the terms of the EU General Data Protection Regulation 2016 and the Regulation of Investigatory Powers (Scotland) Act.

Furthermore, any such recording would breach the principles of dignity and respect, and will be considered to be of a serious and unacceptable nature that is likely to result in disciplinary procedures.

Use of electronic mail

The NES email system (Office 365 Outlook) is a key means of business communication. While emails are often written at speed, staff should be aware that emails constitute formal business communications. Care should be taken that the content is accurate and appropriate, particularly when communicating with external stakeholders. Users should be aware that emails could be disclosable under data protection or freedom of information laws, may form part of the corporate audit trail, and could be considered to constitute a formal instruction or contract. NES staff must never send any e-mail purporting to come from another person

The NES email system must not be used to create, send or forward to other users unsolicited junk or "spam" email, chain letters or otherwise inappropriate or offensive content. Inappropriate, offensive or harassing messages should be reported to line management for consideration under the relevant NES policies.

Consider alternatives to email (such as Yammer, document comment functions, Skype messaging) to reduce the volume of mail messages.

NES staff should comply with any separately provided corporate or local guidance for communication style and email etiquette.

Delegate access

NES email is a corporate communications system and it is vital that email correspondence remains accessible to appropriate staff within NES. Delegate access should be provided to each individual's email account (typically by one's line manager and one or two peers) to ensure that emails can be accessed and actioned in the absence of an individual employee. Where such delegate access arrangements are lacking and where a NES employee is absent from work and access is required to their allocated Office 365 email account for the continuation of work, access will be granted by Corporate Digital Services on the written authority of an appropriate line manager.

Malware and phishing attacks

Emails received by NES can be a source of viruses and other malware, or can be used by attackers to obtain sensitive information. Users must beware of suspicious emails, particularly those with attachments or links. Do not open or download attachments from an email which you are not expecting or follow links. If you have suspicions, contact the Information Governance team on foidp@nes.scot.nhs.uk For confirmed phishing emails, use the *Mark as phishing* option within the Outlook Web Application.

Commercial Webmail

Commercial webmail (such as Yahoo, Hotmail) are not approved for NES business communications. Such systems are insecure, leave no audit trail on NES systems, and are provided for personal and domestic use only: unlicensed business use is a breach of the terms of use.

Auto-forwarding

Auto-forwarding from NES email accounts to external accounts is forbidden for the reasons given above and because of the risk of potentially highly sensitive email traffic being sent unprotected over the internet.

email circulars

The use of circular emails must be sparing and proportionate and only sent out by staff authorised to do so. All-NES, regional or site emails must not be used for trivial or personal purposes. Emails sent to all staff in a region or across NES must not have any attachments, due to the impact on mailbox volumes. Links to documents on Office 365 SharePoint, the intranet or internet may be used instead.

Mailbox management

All staff are responsible for effectively managing the content of their designated Mailbox within Office 365, within the size limits approved by Corporate Digital Services. NES email is provided as a communication tool and should not be used as a general filing system for the storage of documents. Ephemeral email should be deleted as soon as it is read or actioned. Significant email which should form part of an audit trail should be saved to the appropriate SharePoint or OneDrive file or network folder to be part of the relevant corporate record.

Where users are aware of a current or ongoing request for information under the Freedom of Information (Scotland) Act 2002 or the Data Protection Act 1998/GDPR, or of NES involvement in litigation or another formal process, then no emails relevant to the request or process should be deleted until the request or process is resolved.

Staff should take into consideration the pressure on colleagues' mailboxes when sending emails, by using links in preference to attachments, being selective in choosing recipients, and setting expiry dates on time-limited communications.

It is good practice to set an Automatic reply when away from work for more than half-a-ay, where appropriate giving an alternative contact.

Sensitivity of email content

In line with SGHD eHealth Directorate guidance, most information (including personal data) may be sent by email subject to consideration of sensitivity and risk. (For fuller details of the information classification approach, see the Corporate Information Security Policy.)

GREEN: unclassified information

- Such information can be sent to any email address, including via the Internet, to a person or organisation that has a legitimate business need to see.

AMBER: Protected information

- This category includes any information...
- about an individual that would cause short-term distress, inconvenience or significant embarrassment if lost.
- which if lost or disclosed to unintended recipients would lead to a low risk to a person's safety (e.g. loss of an address but no evidence to suggest direct harm would result).
- if lost that would be likely to negatively affect the efficiency of the service.

- Email should only be exchanged between NHS colleagues and trusted partners with a legitimate or legal right to access the information.
- Email should only be sent from official NHSScotland email accounts (i.e. NHS.net or NHS.uk) and not personal non-work related accounts.
- Information in a single email should only relate to one individual as far as possible. Take great care with 'group/circulation addresses' as most privacy breaches are the result of sending to the wrong persons.
- Email can be sent to official organisation email accounts of organisations with which we have regular contact.

RED: Highly sensitive information

- **This category includes any information**
- which if lost could directly lead to actual harm, cause substantial distress and/or constitute a substantial breach in privacy to the subject.
- that affects the privacy or could cause distress to more than one individual
- if lost that is likely to result in undermining confidence in the service or would cause significant financial loss to the organisation, prejudice investigation of crime etc.

- Email can only be exchanged between NHS colleagues and trusted partners with a legitimate or legal right to access the information **and** who are deemed to have adequate network security measures in place
- Email should only be sent from official NHSScotland email accounts (i.e. NHS.net or NHS.uk) and not personal non-work related accounts.
- Email should **not** be used as a medium for communications with unconnected organisations (however, see below regarding Regulatory Bodies), patients or the wider public.
- Information in a single email must only relate to one individual. Take great care with 'group/circulation addresses' as most privacy breaches are the result of sending to the wrong persons.
- Information can only be sent to an official NHS email account (nhs.uk or nhs.net) or partner organisation with GSI. email or equivalence.
- When communicating with UK or Scottish Government agencies, local authorities or the Police, **Red** data must be labelled as **OFFICIAL – SENSITIVE PERSONAL** in compliance with the UK Government security classification scheme**.**

At the time of writing, regulatory bodies (GMC, NMC, GDC, GPhC) are not "connected organisations" within the terms of the current guidance. However, the NES Outlook configuration in Office 365 uses enforced TLS encryption for outgoing email to most domains providing robust protection of the email traffic.

It is clearly vital that NES shares personal data with these bodies regarding the functions of both parties. Further, only a very small proportion of the data NES holds and may be required to share with regulatory bodies, falls within the category of **Red** information. (Examples may be the provision of evidence for fitness to practice hearings.)

NES staff should consider the risks of transferring the specific data and consider the application of controls such as:

- Ensuring that the information is sent to a bona fide official email account of the receiving regulatory body;
- Consider whether the encryption of attachments in transit may be proportionate;
- Use of secure document transfer tools provided by the regulatory body (for example NMC Egress Switch, GMC File Transfer).

For advice or support contact foidp@nes.scot.nhs.uk .

For further information see http://www.ehealth.scot.nhs.uk/wp-content/documents/NHSScotland-Email-Good-Practice-Guide-May-2012.doc.pdf

Internet

Appropriate access to internet resources is vital to support the work for most staff within NES and moderate personal use is permitted where this does not impact negatively on staff performance, network bandwidth or the reputation of NES. Staff are expected to use the internet appropriately. Bear in mind always that when visiting an internet site, information identifying your PC may be logged. Therefore, any activity that is engaged in via the internet may affect NES as an organisation. Staff should not attempt to access internet content which is illegal, offensive or otherwise inappropriate to the workplace.

Staff should never provide their NES e-mail address to websites for non-business purposes (such as on-line shopping or social sites) due to the increased likelihood of "spam" email and hacking attack.

An employee must not deliberately visit, view or download any material from any web site with pornographic content, illegal material or material which is otherwise offensive. If inappropriate material is accessed or downloaded inadvertently, the user should exit the site immediately and the line manager must be informed. Access to a log of internet access may be obtained (on authority of the Head of Corporate Digital Services) if deemed necessary to confirm accidental misuse. This procedure will protect the employee should any trace of inappropriate access be recorded on their device(s) and discovered later.

Internet gateway controls

The Scottish Wider Area Network implements internet gateway controls on behalf of NES and NHSScotland to maintain the integrity of NES systems, protect staff from offensive content or inadvertent illegal activity, maintain availability of bandwidth for business activity and support productivity. NES may apply additional gateway controls.

Sites identified as falling within the following categories may be blocked at the discretion of NES Digital Group:

- Sites promoting pornographic material, incitement to hatred, incitement to violence, gambling;

- Music and other media download sites;
- Internet based email Sites e.g. Hotmail, Google Mail etc.;
- Auction sites.

Requests to have blocked websites made accessible should be submitted through the helpdesk system, flagged as a “Whitelisting Request”.

NES reserves the right to prioritise bandwidth allocation to the delivery of core business systems which may impact negatively on ad hoc or personal internet use.

Clear desk and screen

(ISO27001:2013 11.2.9)

NES has a clear desk/clear screen policy. All NES paper documents (and particularly those containing Red or Amber content) must be locked away in cabinets when not in use.

When leaving your desk, PC monitors must be locked by using the **Ctrl**+**Alt**+**Delete** keyboard combination and then selecting **Lock screen**. You can also use the **Windows**+**L** keyboard combination to automatically lock the screen.

NES Corporate Digital Services may also set a time-out period on NES PCs and laptops so that they lock after a period of inactivity.

Information transfer

(ISO27001:2013 13.2.1)

Where there is a business requirement to share files with non-NES colleagues on an ongoing business basis this can be managed by sharing a folder from NES OneDrive for Business with stakeholders as required.

Sharing and collaboration around documents on an ongoing basis may be managed using a SharePoint online sub-site configured for external sharing.

(Please note that some other NHSScotland organisations may block access to cloud-based tools, for security reasons. This situation is under ongoing review.)

Partner organisations may provide their own tools for secure transfer of files (for example GMC Secure File Transfer and NMC Egress Switch). Where these are available and accredited by the host organisation, they may be used.

Another approved means of securely transferring data is the N3 Secure File Transfer service. Files up to 1Gb can be transferred securely by uploading to the N3 file transfer facility and emailing the link and password to recipients. To use the SFT service the following criteria must be met by both recipient and sender:

- users must have an NHS mail account (required to register)
- users must have registered with the service and have their PIN available
- users must have SWAN connectivity (as staff in NES offices do).

The SFT can be used to transfer any type of data within the size limits. Expected uses are:

- transfer of personal or other sensitive data
- regular but small (<100MB) transfers
- large but one off, ad-hoc data transfers

Please note that the SFT is not designed for large, high volume, regular, data transfers. The SFT service is available at https://nww.sft.nhs.uk

For further guidance see *Online document sharing and storage tools: Good practice guidance for NHS Scotland* 2013. http://www.ehealth.scot.nhs.uk/wp-content/documents/Good-Practice-Online-Document-sharing-tools-March-2013-27-March-2013.pdf For further advice on risk assessment and currently available tools contact foidp@nes.scot.nhs.uk

Faxing

Faxes are an insecure mode of communication and should be avoided for sensitive information where possible. When faxing personal or other sensitive information, precede the fax transmission with a telephone call to the recipient to confirm the fax number, to ensure that someone will be on hand at the machine to receive the fax and seek confirmation from the person that the fax in question been sent has been received.

Identify any numbers that are frequently used and programme these into the machine's "memory dial" facility; equally computer dialling facilities may be used where these are available. Numbers must be tested in conjunction with a telephone call before using the fax to transmit confidential information.

Do not send faxes outside the likely opening times of the office of the recipient.

When a fax including personal or other sensitive information is sent, a front cover must always be used and should always include:

- Name and contact details of the sender
- Details of the intended recipient
- Number of pages in total
- Confidentiality Notice

All NHS organisations maintain "Safe Haven" faxes which are securely managed. These should be used wherever possible.

Mobile devices and teleworking

(ISO27001:2013 6.2, 11.2.6)

Mobile devices present a risk due to the increased potential for theft or loss. NES will manage the risks associated with the use of mobile devices and media in line with the eHealth guidance set out in *Managing Information Assurance for mobile wireless services in NHSScotland: Good Practice Guide* (May 2012).

All NES-owned mobile data storing devices (including USB devices, smartphones, tablets and laptops) will be encrypted to FIPS140 standard. NES will review the encryption software, tools and standards used on a regular basis to ensure compliance with current legal and regulatory standards.

Employee-owned devices such as tablet computers may be used to store or access NES business data and information (including Amber and Red classifications where this has been authorised locally by the employee's line management) under the following conditions:

- The device is enrolled with and partly managed by NES Digital using the Mobile Device Management function within Office 365, which will include;
    - Encryption and configuration of all or part of the device storage;
    - Remote wipe of data and locking of device where necessary;
    - Software distribution;
- The employee undertakes to inform NES Corporate Digital Services immediately if the device is lost;
- The employee agrees to comply with password and other relevant policies and procedures.

NES staff authorised to remotely access NES systems shall comply with all the requirements set out in the associated procedures.

Appropriate authentication methods may be used to control access by remote users, using physical or “soft” tokens allocated to specified users for their sole use and other identity verification factors as instructed in the procedures. The loss of any such token must be immediately reported to Digital Group by the user.

Remote access to Office 365 and online access via portals (such as the NAM Gateway for Web Services, Intranet and Service Now) will be used securely by staff, ensuring that NES documents and data are not downloaded and held on private or public devices, and that other non-NES users of a device do not have access (through saved passwords for example).

When remotely accessing NES Office 365 on a non-NES device, wherever possible files should be edited using the edit in browser option. Where NES documents or data are downloaded onto a non-NES PC or other device, they must be held no longer than necessary on a folder which is not accessible to other users in the household.

NES staff working from home or from public facilities remain responsible for the security of all NES information to which they have access as set out in the NES Homeworking policy. They must:

- Take care to physically protect all NES devices and information assets in their care;
- Ensure that NES documents are not cached or stored on home or public PCs or other devices at the completion of work;
- Ensure all documents or data that have been amended are synced back to the NES network;
- Ensure other household members do not have access to NES data.

Telephony and mobile communications

NES telephone services are provided to support NES business. While essential personal calls are permissible, excessive use of the telephone for personal purposes (such as lengthy private calls or calls to premium rate numbers) is prohibited.

When receiving external phone calls, users must not disclose sensitive information over the phone without taking appropriate measures to confirm the identity and authorisation of the requester. If in doubt, decline to provide sensitive information over the phone and make alternative arrangements using confirmed email or postal addresses.

Mobile devices

Mobile devices such as smart phones are at risk of loss or theft. When not in use, they should be securely locked away. Under no circumstances should they be left in an unattended vehicle (even if locked). These devices are subject to the national policy on mobile computing and must be encrypted if they hold data.

The loss of a NES smart phone must be reported **immediately** to Network Services so that mitigating security actions can be taken.

When in the office all mobile phone ring tones should be set to silent or vibrate.

SMS/MMS messaging

Text messaging may be used to communicate non-sensitive messages to NES staff or service users, such as reminders of deadlines or advice of service issues, as long as the recipients of such messages have signed up to receive them or may have a reasonable expectation that NES will communicate with them in this way.

Given the risks associated with mobile devices, text messaging should not be used to communicate personal data or other sensitive information.

Instant messaging (through Skype for Business) is a corporate tool for rapid communication between NES colleagues. It is not suitable for maintaining an audit trail or

record of discussions, instructions or decisions. Significant communications which require to be placed on record should be made via email.
See also the NHS Scotland guidance: http://www.ehealth.nhs.scot/wp-content/uploads/sites/7/documents/SMS-Good-Practice-Guide-30-August-2012.pdf

Survey and Questionnaire Tools

The approved NES tools for e-questionnaire and survey work are the NES corporate accounts for **Questback** and the **eForms** Service. More information on both can be found here:

http://intranet.nes.scot.nhs.uk/help-me-with/it-related/eforms-and-questback/

Other tools (including freely available web-based survey tools) are **not approved** for NES use, as they reduce the accessibility of surveys and data to the organisation and carry risks around data security and licensing terms of use.

Where third parties conduct surveys on behalf of NES, it may be appropriate for them to use other tools where these are licensed and risk-assessed to the satisfaction of NES.

For further advice on risk assessment contact foidp@nes.scot.nhs.uk

Document control	
Version	1.0 Final version issued
Title	IGP07 User Information Security Policy
Summary	Policy for staff and other users of NES information assets on security. See also IGP04 Corporate Information Security Policy
Date	November 2016
Author	Frank Rankin, Information Governance Manager
Owner	Christopher Wroath, Senior Information Risk Owner
Document No.	IGP07
Document location:	Alfresco DG/Documents/IG/Info Sec/ISMS

Authorisation	
Approved by	Staff Governance Committee
Date of approval	10 November 2016
Date of Issue	21 November 2016
Supersedes	IGP 06 NES eComms Policy, IGP04 Info Sec Policy 2011 (part)
Date for review:	November 2018

Version history

Date	Version	Status/ Summary of changes	Author
Jan 2016	0.1	Initial draft	Frank Rankin
July 2016	0.2	Revision to accommodate Office 365	Frank Rankin
July 2016	0.3	Draft for consultation	Frank Rankin
October 2016	0.4	Submitted to PF	Frank Rankin
November 2016	1.0	Approved by SGC and issued	Frank Rankin

NHS Education for Scotland
Westport 102
West Port
Edinburgh EH3 9DN

tel: 0131 656 3200
fax: 0131 656 3201