	DOCUMENT NO: ENQ-COR-IT-POL-00007	REV: C3

Information Systems Usage Policy

Document Review Cycle

REVIEW PERIOD	NEXT REVIEW	DOCUMENT OWNER
2 Years	Feb 2020	IS & Office Services Manager

EnQuest, Annan House, Palmerston Road, Aberdeen, AB11 5QP, Tel: 01224 975000

Revision History

YYYY	MMM	DD	By	Rev	Detail
2015	Nov	11	S. Potter	A1	
2016	Feb	18	S. Potter	C1	First Issue
2016	May	11	S. Potter	C2	Re-Issue for Use
2018	Feb	08	S. Potter	C3	Minor updates

Revision Change Notices

Rev	Location of Changes	Brief Description of Changes
C2	Section 11	Updated following Legal review by S. Ricketts (General Counsel & Company Secretary)
C3	Document Sign Off Section 4 Section 5 Section 11	Reviewer changed to be A. Talpur who is now Head of Business Services Added 2 bullet points to “users must take care not to” Deleted words and referred to section 11 for consistency Added approval requirement

Document Sign-Off

Signature	Print Name	Position	Date
	Reviewer/Approver Ali Talpur	Head of Business Services	8/01/18
	Author / Document Owner Shaun Potter	IS & Office Services Manager	08/01/18.

CONTENTS

1.0 Introduction

IT Systems play an essential role in the conduct of our business. We use them to manage our business processes and as communication tools. We need to ensure that our IT systems are appropriately protected so that our business process and communication systems are not disrupted or data and information lost.

How we communicate with people not only reflects on each individual but also on the organisation. We value our ability to communicate with colleagues, clients and business contacts, and we invest substantially in information and communications systems, which enable you to work more efficiently. We trust you to use them responsibly.

EnQuest's IT Systems are made available for the purposes of the business. Limited and responsible personal use is permitted. The use of IT Systems is governed by the terms of this policy. A failure to adhere to this policy may result in an increased risk of business disruption, loss of data or information, the curtailment or withdrawal of IT Services to an individual, investigation and possible disciplinary action.

Please read this policy carefully. If you have any queries as to the contents then please speak to your line manager or regional IT Service Desk.

2.0 Scope and Applicability

Document Hierarchy

EnQuest's Information Security Policies consists of four main documents, these are supported by regional processes and operating procedures.

- **An overarching Information Security Policy** - This is a high level document that reflects Executive Management's requirements regarding Information Security. This document has been authorised by the Chief Executive and is applicable to all regions and countries
- **Information Systems Security Policy** - Contains detailed requirements regarding the design, procurement, configuration, maintenance and operation of IT Systems. Whilst a generic framework will be utilised there will be regional variations to reflect local regulation and practice
- **This Information Systems Usage Policy** - Addresses specific risks arising from people handling information and using information systems. Whilst a generic framework will be utilised there will be regional variations to reflect local regulation and practice
- **Data Protection Policy** – Specifically underlines our commitment to keeping data safe. Whist a generic framework will be used there will be regional variations to reflect local regulation and practice

Applicability

This Policy applies to:

- all permanent, temporary and contract workers employed or engaged by EnQuest, its subsidiaries or any 3rd party organisations and supply chain partners who have access to information, data and to information systems that are part of EnQuest business. All of these parties are referred to as "users" for the purpose of this document.
- EnQuest business specific IT Systems including those supporting Corporate and Control systems. Where IT systems are provided for welfare, guest, or bring your own device (BYOD) connectivity and this is physically or logically separate from the business network, a lower standard of security may be applied based on a current risk assessment.

For the purposes of this document the term "IT Systems" are defined as all physical and logical information assets including hardware, middleware, software, applications, network and network equipment, telephones and telephony systems, data, information and related processes.

Compliance

- Any employee found, after investigation, to have deliberately or negligently violated the requirements of this Policy may be subject to disciplinary action, up to and including termination of employment.
- At its sole discretion, EnQuest may require the removal of any other user who is found to have deliberately or negligently violated the terms of this policy from its service.

Accountabilities

All users are accountable for following this policy and for reporting any compromise or breach of the policy.

The Regional IS Manager is accountable for:

- ensuring that security risks are continuously assessed
- deploying appropriate preventative, monitoring, detection and reactive tools and practices to mitigate that risk
- having reasonable tools, processes and practices in place to respond to and resolve any security related incident.

3.0 General Security

In order to protect our IT Systems all users **must** use IT Systems:

- sensibly, professionally and lawfully
- in a manner consistent with their business role and duties
- treat all information relating to business operations with appropriate care and diligence; this includes both paper-based and electronic information
- treat all information relating to clients and business operations as confidential

And **must not**:

- make any attempt to disable, modify or bypass any security measures
- attempt to install any software or take an action that might install software, hardware (including wireless networks) or other IT Systems without the authorisation of the IS department
- access or seek to access data or information or systems for which you are not authorised
- carry out any activity that you believe may unnecessarily degrade the performance of or prevent access to any IT System
- carry out any activity that is for personal financial gain
- communicate political views or opinions
- do or say anything which would be subject to disciplinary or legal action
- access, use, make or send any discriminatory, defamatory comment on the grounds of a person's sex, race, disability, age, sexual orientation, religion or belief
- use make or send material that is designed to be, or could be construed as, bullying or harassment by the recipient
- access, use, make or send any material that is obscene, sexually explicit, defamatory, may incite or depicts violence, or describes techniques for criminal or terrorist acts or other offensive or unlawful material
- copy any software, data, information or other copyrighted material such as photographs, music, books, videos or other resources for which EnQuest or the end users are not appropriately licensed and has not been approved by the IS Team.

4.0 Username and Password

Authorised user access to IT Systems is gained through the use of a username and secure password.

Except for shared accounts the username and password is provided to a specific user who has been authorised to access EnQuest IT Systems. If a user password is shared with any other person or a device is left unattended after a user has logged in then our basic security is compromised and unauthorised and unidentifiable individuals can access our systems with the potential to authorise business processes, copy, delete, edit data and cause disruption to our IT Services.

Users are accountable for all activity that occurs under their issued username; the password is the manner that restricts access. Users must therefore take care **not to**:

- Share passwords with anyone, including peers, assistants, superiors, family members or the IT service desk
- Use a password that would be easy to guess
- Use a password that is used for other services (password must be unique)
- Discuss or talk about a password in front of others, including any hint at the format of a password
- Reveal a password on any questionnaires
- Reveal a password to co-workers providing holiday or absence cover
- Write passwords down
- Store unencrypted passwords in a file on ANY computer system or media

- And **must** Report any attempt that has been made by anybody to discover password information, to the IT Service Desk
- Immediately change a password if there is any cause to suspect that it may have been compromised
- Advise the IT Service Desk immediately if there is any cause to suspect that the password may have been compromised.

If a legitimate business requirement exists for another user to access IT Systems that they cannot currently access, including user E-mail accounts or “personal” storage areas then they should contact the IT Service Desk who will enable that access for the individual under their own username and password.

Users who are members of shared accounts must only share the password for that account with other approved members of that group.

5.0 E-mail

EnQuest E-mail is a primary business communication system. E-mails can, however, compromise the security of IT services through carrying hidden disruptive code within attachments and, if not used carefully, could lead to company reputation issues. Incidental and occasional personal use is permitted, subject to the restrictions contained in this policy.

When using E-mail users **must**:

- ensure that the appropriate approvals are in place before making any business commitments in an E-mail

And must **not**:

- Delete, alter or modify E-mail for the purpose of deceiving or misleading anyone
- Send information that is Sensitive, Confidential or contains any personal information to external recipients in the body text of an E-mail. If this information must be sent it should be in an attachment. Consideration must be given to encrypting and password protecting that document. The IT Service Desk can provide advice as required.

- Send E-mails that contain words or material that could damage the reputation of EnQuest, its employees, stakeholders or partners or be considered unlawful. Something, which you may consider as 'harmless fun', may well offend someone else and so should be avoided.
- use auto-forwarding functionality from EnQuest to external addresses as this is prohibited
- use your business E-mail address for non-business activities such as internet banking, online shopping or social media sites
- forward, create or send unsolicited E-mail messages that contain chain letters, 'junk mail' or other advertising material that have no business purpose.

And must be aware:

- That E-mails are legally binding and can be used as evidence in civil and criminal proceedings
- That E-mail is not a guaranteed delivery service and is not a form of instant communication.
- That EnQuest reserves the right to access an individual user's E-mail account as outlined in section 11 of this Policy
- That EnQuest automatically adds a legal disclaimer to the foot of all externally sent E-mail.

And care must be taken when:

- you copy an E-mail to others if it reveals all the recipients' E-mail addresses to each recipient (e.g. in the case of marketing and mailing lists) as it may breach the Data Protection Act
- "replying to all" on an E-mail with a large distribution list.

And it is strongly recommended that:

- When a user plans to be absent from work that they apply an 'Out Of Office' notice to their E-mail account
- To mark all personal E-mails sent by marking the subject heading as "PERSONAL" and filing any personal E-mail messages in a mailbox folder marked PERSONAL.

6.0 Internet

The internet is a useful source of business information. However, it contains many methods that can be used to compromise the security of IT services (through capabilities to download harmful code and programmes when certain sites are accessed or files downloaded). Users must be careful and apply good sense to their internet activity to prevent a security breach. Incidental and occasional personal use is permitted, subject to the restrictions contained in this policy and line management agreement.

When using the internet you must not:

- Allow personal use to interfere with your or your colleagues' work performance.

Be aware:

- that when visiting a website, information identifying your PC may be logged by the website owner. Do not visit sites that may be harmful to your or EnQuest's reputation
- that the frequency, length of time and type of Internet usage appropriate to an individual's job is for the individual and their line manager to determine
- that EnQuest, as a reputable operator
    - operates controls to automatically detect and block access to information that is obscene, sexually explicit or defamatory, may incite or depict violence, describes techniques for criminal or terrorist acts and subjects that would normally be inappropriate for business use. The "blocked" list is provided by third parties and is constantly updated; however, it is not going to block everything. If you do

    - accidentally access inappropriate material that has not been blocked please contact the IT Service Desk who will add the site to the blocked list.
    - Routinely monitors and logs all internet traffic. Managers may be provided with a historical log if there is reasonable cause to do so.
- if you find that you need access to a site that has been blocked for the purposes of carrying out your business duties then contact the IT Service Desk who can remove this site from the blocked list if appropriate.

7.0 Social Media Use Requirement

Social Media which includes interactive online media that allows parties to communicate instantly with each other or to share data in a public forum (e.g. Twitter, Facebook, LinkedIn, blogs etc.) is a growing tool used to share information, find people, share personal and business information, join professional discussions and organizations and help resolve business problems. It is also a tool that can be used to compromise security in a similar manner to the internet but also through gaining personal information about individuals that can be used to gain information that may be confidential about the user's work and used target their work IT Systems.

Users must be very careful when using Social Media platforms whether on EnQuest IT Systems or personal systems as it is easy to lead others to believe that you are representing the company or provide information that is not for public consumption.

Users must not:

- Use any EnQuest related entity name as a header in any discussion or profile
- Represent or claim to represent EnQuest unless authorized to do so
- Reveal any company information that is not in the public domain or publish any EnQuest document unless authorized to do so by appropriate persons
- Reveal trade secrets or information owned by any business within EnQuest
- Give away confidential information about an individual (such as a colleague or customer contact) or organisation (such as a partner business)
- Discuss EnQuest's internal workings (such as deals that it is doing, bids being worked on, or its future business plans that have not been communicated to the public)
- Make any statement that may bring EnQuest into disrepute, for example by:
    - Criticising or arguing with customers, colleagues or rivals
    - Making defamatory comments about individuals or other organisations or groups
    - Posting images that are inappropriate or link(s) to inappropriate content

8.0 Telephony Systems

EnQuest provides desktop phones to most users and mobile phones and tablets which are often "smart" devices where there is a strong business case. They are provided for business purposes. A very limited amount of personal usage is tolerated (incoming and outgoing calls). Additionally EnQuest allows users to connect their personal "smart" phones to particular EnQuest services allowing the user to access that service when out of the office.

Users must:

- Ensure that all telephone calls made using EnQuest devices are done so in a professional manner
- Ensure that they are aware of the cost of the calls they are making and take all reasonable measures to manage the cost of those calls prudently
    - For international travel, use internet based phone services wherever possible
    - Contact the IT Service Desk to ensure that the most effective mobile contract is in place for the travel destination
    - For international calls from landlines consider using internet based telephone services, particularly for calls which are not business related
- be aware of the environment in which calls are made; for example, confidential information should not be discussed in public places
- be aware that EnQuest may recover personal call and data costs from a user

9.0 Tidy Desk and Clear Screen

Many individuals have legitimate access to EnQuest offices, including, cleaners, service professionals and visitors. Individuals must not have access to sensitive, confidential or personal information that they are not entitled to see. Consequently, no sensitive, confidential or personal information or data should be left unattended on a desk. For this reason EnQuest has adopted both a Tidy Desk and Clear Screen Policy to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours or when work areas and computers are unattended.

Users must ensure that:

- paper and computer media containing information which is confidential, sensitive or contains any personal details are stored in suitable locked cabinets or other forms of security furniture when not in use.
- sensitive, confidential or personal information or data is cleared from printers, faxes and photocopiers as soon as possible and, when no longer required, destroyed in a secure manner.
- information which is sensitive, confidential or personal will not be held on a reception desk within reach or sight of visitors.
- when vacating meeting rooms or shared space, any information or data, regardless of format, is removed and all whiteboards are cleared and used flipchart pages are removed and disposed of securely.
- computer screens are 'locked' or logged out before leaving any workstation unattended.

10.0 Mobile Equipment

Mobile computing enables flexible working practices that increase efficiency. However, it also creates specific information security issues as the loss of or theft of a mobile IT device could potentially lead to:

- The disclosure or loss of information. If a mobile IT device is lost or stolen, then any information on it which has not been backed up cannot be recovered
- Unauthorised access to EnQuest IT systems - A mobile IT device that is configured to access EnQuest's networks and resources could represent a significant threat in the wrong hands
- The loss of valuable equipment - Mobile-computing devices have an intrinsic value, as well as the costs incurred in configuring replacement devices etc.
- Potential consequences to individuals – for example a smashed car window or violent assault during the theft of a device.

Following an approved business case, EnQuest's IS department will provide suitable mobile IT equipment. All such devices will have data encryption implemented and will require an appropriate username and password.

Mobile equipment supplied by EnQuest IT is for the sole use of the individual it is issued to and access is not to be shared.

Users must ensure:

- that data is backed up on a periodic basis as appropriate to the importance of the data. This is the responsibility of the end user, please contact the service desk for help to do this.
- Care is taken when IT equipment is used in a public place, such as train or hotel, to ensure the information on display cannot be overlooked or read by those around them.
- That mobile equipment is secured in locked furniture when left overnight or for extended periods in EnQuest offices
- equipment is not left unattended in public places
- that mobile devices are not left in a car overnight

- if it is necessary to leave equipment in a vehicle that it is in the boot or load space and is not visible
- The actual or suspected loss or theft of the mobile device is reported to the IT Service Desk and line manager
- Ensure that a mobile device is not used for:
    - Excessive Personal use
    - Storing personal information, images or data;
    - Installing software or applications (apps) that are not licenced
    - The long-term storage of EnQuest data.

EnQuest provided portable equipment must be returned to the IS department for any configuration, repair or support issue.

11.0 Access to Information and Data

EnQuest is ultimately responsible for all communication, data and information held on or transmitted through its IT systems and network. As far as appropriate, EnQuest will respect your privacy and autonomy whilst working; however EnQuest may, subject to the approval of the Head of Business Services, HR Manager, General Counsel or Director, and in accordance with applicable data protection and regulatory requirements, authorise and allow another employee, manager or third party to read any information, data and communication in any account without notice at its discretion. Circumstances may include:

- Finding and providing evidence of business transactions
- Ensuring that EnQuest business procedures, policies and contracts have been adhered to
- Checking compliance with legal obligations
- Monitoring standards of service, staff performance, and for training
- Detecting unauthorised use of EnQuest systems, including criminal activity
- Accessing information, data or communication in a user's absence, leave, sickness or any other reason
- Accessing information, data or communication if a user is absent or no longer working for the company.

In the event of an investigation into any disciplinary or criminal behaviour access may be unlimited and include files and folders marked as personal.

12.0 IT Service Monitoring and Reporting

In order to protect IT Services and infrastructure it is essential to implement a level of monitoring that will help prevent and detect:

- Unauthorised access
- Abnormal activity that may represent a threat (proliferation of files, abnormal document movement, increased unexplained resource usage may be due to a virus or other intrusion)
- capacity, performance or usage issues
- Attempts to create denial of service issues.

IT systems monitoring is carried out by EnQuest authorised personnel as permitted by local legislation. This allows the monitoring of systems and network traffic without consent for legitimate purposes such as:

- Safeguarding the integrity of EnQuest's information and information systems
- Recording evidence of transactions
- Policing regulatory compliance
- Detecting crime or unauthorised use.

Users should be aware that:

- EnQuest provided E-mail and internet service usage is logged and reports can be made available on its use to an individual level should a legitimate request be made
- reporting and inspection of a specific individual worker's activities, where the worker is unaware and has not given permission for it to take place, is only permitted where written authorisation has been granted by EnQuest's IT and HR Manager
- Information obtained by or on behalf of EnQuest from the monitoring or lawful interception of E-mail and Internet use will be stored securely and kept for no longer than is necessary.

Please refer to our Data Protection Policy for more information on how we protect our data.

13.0 Disposal of IT Equipment

All IT equipment must be returned to the IS team for disposal. The IS team will ensure that all data is removed and cannot be recovered.

Attachment 1 – Declaration

Information Systems Usage Policy Declaration (ENQ-COR-IT-POL-00007)

I …….. (Please Print Name) have read the EnQuest Information System Usage Policy and accept the terms therein. I am aware that this policy may be updated and amended from time to time and that the latest version will be available on the EnQuest Business Management System. I will familiarise myself promptly with any change to this policy.

Signed ……

Date …….