

Information Technology
ENQ-COR-IT-POL-00007

THIS DOCUMENT IS CLASSIFIED AS CRITICAL

Information Systems Usage Policy



APPLICABILITY: 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.


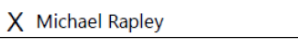
Document Owner	Global Cyber Security Manager				
Legacy Number					
Revision	C6	Issue Date	15 June 2020	Next Review Date	27 Mar 2022

Information Systems Usage Policy

Revision History

Rev	Reason for Issue	Created By	Job Title	DD	MM	YYYY
A1	For review	S. Potter	IS & Office Services Manager	11	11	2015
C1	First Issue	S. Potter	IS & Office Services Manager	18	02	2016
C2	Re-Issue for use	S. Potter	IS & Office Services Manager	11	05	2016
C3	Minor updates	S. Potter	IS & Office Services Manager	08	02	2018
C4	Additional line to section 5.	S. Potter	IS & Office Services Manager	19	04	2018
C5	Policy re-issued in new Template.	M. Rapley	Global Information Risk Manager	27	03	2020
C5	Minor revisions	M. Rapley	Global Information Risk Manager	27	03	2020
C6	Minor revisions	M. Rapley	Global Cyber Security Manager	15	06	2020

Signatories:

Rev	Print Name	Job Title	Signature
C6	Reviewed By Michael Thomson	IT Manager	<div style="text-align: right;">06/07/2020</div>  Michael Thomson Signed by: Thomson, Michael
C6	Approved By Michael Rapley	Global Cyber Security Manager	<div style="text-align: right;">30/06/2020</div>  Michael Rapley Signed by: Rapley, Michael

Revision Change Notices

Rev	Location of Changes	Brief Description of Changes
C2	All Document	Updated following Legal review by S. Ricketts (General Counsel and Company Secretary)
C3	Reviewer Section	Reviewer changed to be A. Talpur who is now Head of Business Services
C3	Section 11	Added 2 bullet points to "users must take care not to" Deleted words and referred to section 11 for consistency Added approval requirement
C4	Section 5	Added line to be clear that adding external email accounts to EnQuest devices or systems is not permitted (security recommendation)

Information Systems Usage Policy

C5	All Document	Policy re-issued in new Template.
C5	Reviewer Section	Policy re-issued in new Template. Global Information Risk Manager now document owner. Ali Talpur, Michael Thomson and BK Foo added as reviewers
C6	Signatories	Updated job descriptions to reflect org charts approved for Transformation 2020. Full sign off will occur in the next review period. Two signatories are sufficient for this revision in line with Transformation 2020 guidance.

Information Systems Usage Policy

Electronic Distribution:		
SNO	Contact / Name	Email Address
1		
2		
3		
4		
5		
6		
7		
8		

CONTENTS

1.0	Introduction	6
2.0	Scope and Applicability	6
3.0	General Security	7
4.0	Username and Password	7
5.0	Email	8
6.0	Internet	9
7.0	Social Media Use Requirement	10
8.0	Telephony Systems	10
9.0	Tidy Desk and Clear Screen	10
10.0	Mobile Equipment.....	11
11.0	Access to Information and Data.....	11
12.0	IT Service Monitoring and Reporting.....	12
13.0	Disposal of IT Equipment	12

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, regional IT Service Desk, or the Global Cyber Security Manager.

2.0 Scope and 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 violate the requirements of this Policy might 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 Global Cyber Security 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**:

- 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 IT department.
- Access or seek to access data, 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 that may 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 IT Team.

4.0 Username and Password

Authorised user access to IT Systems is gained via 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 cause harm to EnQuest.

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**:

Information Systems Usage Policy

- Share passwords with anyone, including peers, assistants, superiors, family members or the IT service desk.
- Use a password that is 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.
- Inform 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 Email

EnQuest E-mail is a primary business communication system. E-mails can 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.
- Send E-mails that could be considered unlawful.
- Use auto-forwarding functionality from EnQuest to external addresses as this is prohibited.

Information Systems Usage Policy

- 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.
- Add, or attempt to add, external E-mail accounts onto EnQuest provided equipment or services.

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.
- 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 GDPR requirements.
- "Replying to all" on an E-mail with a large distribution list.

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. 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.
- EnQuest routinely monitors and logs all internet traffic. Managers may be provided with a historical log if there is reasonable cause to do so.

Information Systems Usage Policy

- If you find 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 it is appropriate.

7.0 Social Media Use Requirement

Social Media use is governed via the Social Media Use policy owned by the Communications Department. This Policy can be found on BMS.

8.0 Telephony Systems

EnQuest provides desktop phones to most users. Users are provided 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. In addition, 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 it hosted 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 IT 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 office.
- 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 IT 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.

Information Systems Usage Policy

EnQuest will respect your privacy and autonomy whilst working. However, EnQuest may, subject to the approval of the Global Business Services Director, HR Manager, or General Counsel, 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 an EnQuest 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.

13.0 Disposal of IT Equipment

All IT equipment must be returned to the IT team for disposal. The IT 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