# Information Security Policy

## Table of Contents



## Document Control

| AUTHOR | VERSION | ISSUE DATE | DESCRIPTION |
|---|---|---|---|
| Lucy Hayes | DRAFT | 9th May 2019 | Initial Review |
| Lucy Hayes | V0.1 | 9th May 2019 | Final Review |
| Lucy Hayes | V1.0 | 17th May 2019 | Release |
| Lucy Hayes | V1.1 | 01st April 2021 | Review |
| Lucy Hayes | V1.2 | 25th November 2022 | Review |
| Lucy Hayes | V1.3 | 01st April 2023 | Review |
| Lucy Hayes | V1.4 | 31st March 2024 | Review |

# INTRODUCTION

This policy is concerned with the management and security of the Q3 Facilities Holdings Limited ('Q3') and any associated group company information assets (an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to Q3 and the use made of these assets by its members and others who may legitimately process Q3 information on behalf of the Q3.

This overarching policy document provides an overview of information security and may list a hierarchical set of policy documents (sub-policies) which taken together constitute the Information Security Policy of Q3.

This policy applies to all employees, contractors, temporary workers and suppliers ('users') of Q3 who have access to computers, mobile devices and or the Internet to be used in the performance of their work.

## Purpose

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

## Scope

The documents in the Information Security Policy set apply to:-

- All building, sites & offices including any location where a user undertakes activities on behalf of Q3
- Any information assets which are owned by he Q3 or any asset or device are connected to any networks managed by Q3.

The documents in the Information Security Policy set apply to all information which Q3 processes, irrespective of ownership or form. The documents in the Information Security Policy set apply to all members of Q3 and any others who may process information on behalf of Q3.

## Structure

This top-level document lists a set of other sub-policy documents which together constitute the Information Security Policy of the Q3. All of these documents are of equal standing. Although this policy set should be internally consistent, for the removal of any doubt, if any inconsistency is found between this overarching policy and any of the sub-policies, this overarching policy will take precedence.

Each of the sub-policy documents only contains high-level descriptions of requirements and principles. They do not and are not intended to include detailed descriptions of policy implementation. Such details will, where necessary, be supplied in the form of separate procedural documents which will be referenced from the relevant, individual sub-policy documents.

### Information Security Principles

Q3 has adopted the following principles, which underpin this policy:

- Information will be protected in line with all relevant Q3 policies and legislation, notably those relating to data protection, GDPR, PII, human rights and freedom of information.
- Information will be made available solely to those who have a legitimate need for access.
- All information will be classified according to an appropriate level of security.
- The integrity of information will be maintained.
- It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
- Information will be protected against unauthorised access.
- Compliance with the Information Security policy will be enforced.

### Governance

Responsibility for the production, maintenance and communication of this top-level policy document and all sub-policy documents lies with Q3's directors.

This top-level policy document has been approved by the Q3 directors.

Substantive changes may only be made with the further approval of directors. Responsibilities for the approval of all sub-policy documents are the responsibility of the directors. Before approving any sub-policy, the directors may consult with external risk management professionals, Senior User Groups and/or other groups as appropriate.

Each of the documents constituting the Information Security Policy will be reviewed annually. It is the responsibility of the directors to ensure that these reviews take place. It is also the responsibility of the directors to ensure that the policy set is and remains internally consistent.

Changes or additions to the Information Security Policy may be proposed by any member of staff, via their appropriate line manager.

Any substantive changes made to any of the documents in the set will be communicated to all relevant personnel.

### Documentation Set

- Security Policy
- CCTV Policy
- Equipment Policy
- Bring Your Own Device Policy
- Internet Usage, Email and Social Mead Usage Policy & Guidelines
- Removable Media Policy
- Encryption Policy
- Messaging Policy
- Privacy Policy - https://www.q3services.co.uk/legal-notice1

All Users are required to acknowledge receipt and confirm that they have understood and agree to abide by the policies herein.

## Training

Overall responsibility for the Information Security Policy lies with the Operations director who has responsibility for overseeing the development and implementation of operational procedures.

Staff may receive training regarding the policies from a number of sources:

- policy/strategy and procedure manuals;
- line management;
- specific training course;
- team meetings; and
- SharePoint.

Staff will be made aware of procedural document updates as they occur via team huddles, team meetings, staff bulletins and staff briefings.

## User compliance

I have read and understood and will abide by this Information Security Policy. I further understand that should I commit any violation of this policy; my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

| _____ | _____ | _____ |
|---|---|---|
| Name | Signature | Date |

# SECURITY POLICY

## Introduction

This policy deals with both physical & logical access to Q3. Q3 provides its users with equipment which may also include a work area in order to carry out daily duties and access authorised systems, services & physical sites.

This provides our users with a clear policy direction that requires them to protect Q3 premises and assets and ensure that all necessary physical protective security measures are in place to prevent unauthorised access, damage and interference to Q3 assets and the occupants of its premises.
The policy is to establish a standard for management across Q3 to ensure the protection of physical sites, services, systems and the protection of those assets and the frequency of change.

## Scope

The scope of this policy includes all users who have access to an Q3 site and/or systems.

The purpose of this policy is to provide a framework and procedures for identifying and dealing with security risks facing Q3, its users and visitors. This policy will allow Q3, in as far as is reasonably practicable, to ensure the safety and security of Physical & Logical assets.

## Physical Security

In general terms, physical security means the positioning of physical and procedural obstacles to prevent unauthorised access to buildings and other physical assets. This policy specifically addresses the responsibilities and governing framework for the management, installation and maintenance of the following:

- Intruder Alarm Systems including area surveillance sensors, volumetric sensors, high security perimeter protection, infra-red devices, etc.
- Access Control Systems including card systems, fobs, keys, biometrics, turnstiles, trap doors, etc.
- Closed Circuit Television (CCTV) Systems including video surveillance, cameras, 360-degree surveillance domes, switching, matrices, IP video, digital recording, image analysis, privacy zone protection, etc.
- Appropriate controls to ensure the safety of users and visitors.

Physical Security will also involve a balance between physical presence and use of technology. The level of physical presence, e.g. patrols and guarding, is an ongoing evaluation/assessment and the use of technology will require constant monitoring to ensure it is working and operating as intended.

## Users

We expect our Users to observe the following principles:

- Do not give your keys to any unauthorised user.
- Any door access capability, such as a fob or pass is for the express usage of the assigned user only.
- Codes for alarm and control panels should not be divulged without the authorisation of a director
- Users must always wear your id badge on Q3 premises
- Challenge all people whom are not wearing a badge or visitors pass, or any unaccompanied visitor.
- Remove your badge and secure in a safe place once you leave the premises.

## Visitors

The following rules apply for all kinds of visitors:

- Visitors should sign in and show some form of identification.
- Visitors will receive passes and return them once the visit is over.
- Employees must always tend to their visitors while they are inside our premises and ensure the correct personal protective equipment is always worn.
- Our internet usage and data protection policies temporarily cover our visitors while they are on company premises. They must not misuse our internet connection, disclose confidential information or take photographs of restricted areas. If they don't conform, they may be escorted out or face prosecution if appropriate.
- Visitors are allowed during working hours. After-hours visitors must have written authorization from the directors.
- As a general rule, employees may not allow access to our sites to unauthorised personal visitors. We can make exceptions on a case-by-case basis after obtaining authorisation from a director.
- Contractors, suppliers and service vendors, like IT technicians and plumbers, can enter our premises only to complete their job duties. Front-desk employees are responsible for providing contractors and vendors with passes and for instructing them to wear those badges at all times on our premises.
- Our company may occasionally accept the following types of visitors. Student, Investors, Customers, Job candidates & Business Partners. These visitors should receive written authorization from HR or management before entering our premises.

## Logical Security

Logical Security consists of software safeguards for an organisation's systems, including user identification and password access, authentication, access rights and authority levels. These measures are to ensure that only authorised users can perform actions or access information.

## General

- Windows hello is deployed on Q3 Desktops & Laptops and requires you to set up a PIN and the option of facial recognition if supported by your device.
- Screen locks are deployed on all Windows machines and come into force after 5 minutes of inactivity.
- Multi-Factor-Authentication (MFA) is deployed for all O365 users and requires the user to register a mobile number and or email address to protect your account.
- All mobile devices must be protected with a six-digit PIN
- Mobile devices will be wiped after 10 incorrect PIN attempts
- Individual user names and or passwords are not to be shared under any circumstances
- Generic usernames and or passwords are only for authorised users and should not be communicated to other users without express consent.
- All systems-level passwords (e.g., root, enable, administrator, application administration accounts, etc.) must be complex.
- All production system-level passwords must be part of the Information Security administrated global password management database.
- All user-level passwords (e.g., email, web, desktop computer, apps, etc.) must be changed at least every 90 days and cannot reuse the past 6 passwords.
- User accounts with access to admin privileges must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.

- All user-level, system-level, and admin access level passwords must conform to the guidelines described below.

## Password Construction Requirements

- Be a minimum length of twelve (12) characters and must include a special, uppercase and numeric character.
- Check prospective passwords against a list that contains values known to be commonly used, expected, or compromised.
- Avoid keeping a record (e.g. on paper, software file or hand-held device) of secret authentication information unless this can be stored securely and the method of storing has been approved (e.g. password vault)
- Do not use the same secret authentication information for business and non-business purposes
- Not be a dictionary word or proper name.
- Not be the same as the User ID.
- Expire within a maximum of 90 calendar days unless the account is protected by MFA
- Not be identical to the previous ten (6) passwords.
- Not be transmitted in the clear or plaintext outside the secure location.
- Not be displayed when entered.
- Ensure passwords are only reset for authorised user.

## Protection Standards

Do not use your User ID as your password. Do not share Q3 passwords with anyone, including IT, administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Q3 information.
Here is a list of “do not’s”

- Don’t reveal a password over the phone to anyone
- Don’t reveal a password in a email message
- Don’t reveal a password to the boss
- Don’ talk about a password in front of others
- Don’t hint at the format of a password (e.g., “my family name”)
- Don’t reveal a password on questionnaires or security forms
- Don’t share a password with family members
- Don’t reveal a password to a co-worker while on vacation
- Don’t use the "Remember Password" feature of applications
- Don’t write passwords down and store them anywhere in your office.
- Don’t store passwords in a file on ANY system unencrypted.

If someone demands a password, refer them to this document or have them call the Information Security Officer.

If an account or password is suspected to have been compromised, report the incident to IT Support and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the IT Team. If a password is guessed or cracked during one of these scans the user will be required to change it.

## Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

- When a user retires, quits, is reassigned, released, dismissed, etc.
- Default passwords shall be changed immediately on all equipment.
- Contractor accounts, when no longer needed to perform their duties.

**Risks/Liabilities/Disclaimers**

Any user found to have violated this policy may be subject to disciplinary action and prosecution in a court of law.

# CCTV POLICY

## Introduction

This Policy seeks to ensure that the Close Circuit Television (CCTV) system used at London Q3 is operated in compliance with the law relating to data protection (currently the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA 2018")) and includes the principles governing the processing of personal data in our data privacy policy.

It also seeks to ensure compliance with privacy law. It takes into account best practice as set out in codes of practice issued by the Information Commissioner and by the Home Office. Q3 therefore uses CCTV only where it is necessary in pursuit of a legitimate aim, as set out below and only if it is proportionate to that aim.

Q3 seeks to ensure, as far as is reasonably practicable, the security and safety of all assets, staff, visitors, contractors, its property and premises.

## Q3 therefore deploys CCTV to:

- Promote a safe Q3 community and to monitor the safety and security of its premises;
- Assist in the prevention, investigation and detection of crime;
- Assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings; and assist in the investigation of breaches of its policies by staff, visitors and contractors and where relevant and appropriate in investigating complaints.

## Scope

This policy applies to CCTV systems in all sites & buildings where Q3 has a presence.

This policy does not apply to any Webcam systems located in meeting rooms, which are used for the purposes of monitoring room usage and to assist with the use of the audio-visual equipment.

This policy applies to all Q3 staff, contractors and agents who operate, or supervise the operation of, the CCTV system.

## General

The CCTV systems installed in and around Q3's estate cover building entrances, car parks, perimeters, external areas such as courtyards, internal areas such as social spaces, computer rooms, rooms with high value equipment, some corridors and reception areas. They continuously record activities in these areas and some of the cameras are set to motion detection.

CCTV Cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities etc.

CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed where relevant, so that staff, contractors, visitors and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

The contact point indicated on the CCTV signs around Q3 should be available to members of the public during normal business hours. Employees staffing the contact telephone number point must

be familiar with this document and the procedures to be followed in the event that an access request is received from a Data Subject or a third party.

### Covert recording

Covert recoding (i.e. recording which takes place without the individual's knowledge):

- May only be undertaken in exceptional circumstances, for example to prevent or detect an unlawful act or other serious misconduct, and if is proportionate i.e. there is no other reasonable, less intrusive means of achieving those purposes;
- May not be undertaken without the prior written authorisation of a director. All decisions to engage in covert recording will be documented, including the reasons;
- Will focus only on the suspected unlawful activity or suspected serious misconduct and information obtained which is not relevant will be disregarded and where reasonably possible, deleted; and will only be carried out for a limited and reasonable period consistent with particular purpose of the recording and will not continue after the investigation is completed.

### Processing of Recorded Images

CCTV images will be displayed only to persons authorised to view them or to persons who otherwise have a right of access to them. Where authorised persons access or monitor CCTV images on workstation desktops, they must ensure that images are not visible to unauthorised persons for example by minimising screens when not in use or when unauthorised persons are present.

Workstation screens must always be locked when unattended.

### Quality of Recorded Images

Images produced by the recording equipment must be as clear as possible, so they are effective for the purpose for which they are intended.

- Recording features such as the location of the camera and/or date and time reference must be accurate and maintained;
- Cameras must only be situated so that they will capture images relevant to the purpose for which the system has been established;
- Consideration must be given to the physical conditions in which the cameras are located i.e. additional lighting or infrared equipment may need to be installed in poorly lit areas;
- Cameras must be properly maintained and serviced to ensure that clear images are recorded, and a log of all maintenance activities kept; and as far as practical, cameras must be protected from vandalism in order to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit within a vandal resistant casing.

### Retention and Disposal

CCTV images are not to be retained for longer than necessary, taking into account the purposes for which they are being processed. Data storage is automatically managed by the CCTV digital records which overwrite historical data in chronological order to produce an approximate 28-day rotation in data retention.

Provided that there is no legitimate reason for retaining the CCTV images (such as for use in disciplinary and/or legal proceedings), the images will be erased following the expiration of the retention period.

**All retained CCTV images will be stored securely.**

## Third Party Access

Third party requests for access will usually only be considered in line with the GDPR and DPA 2018 in the following categories:

- Legal representative of the Data Subject;
- Law enforcement agencies including the Police;
- Disclosure required by law or made in connection with legal proceedings;
- HR staff responsible for employees in disciplinary and complaints investigations and related proceedings.

Legal representatives of the Data Subjects are required to submit to Q3 a letter of authority to act on behalf of the Data Subject and the subject access request together with the evidence of the Data Subject's identity.

The Data Protection and Information Compliance Officer will disclose recorded images to law enforcement agencies including the Police once in possession of a form certifying that the images are required for either: an investigation concerning national security; the prevention or detection of crime; or the apprehension or prosecution of offenders, and that the investigation would be prejudiced by failure to disclose the information. Where images are sought by other bodies/agencies with a statutory right to obtain information, evidence of that statutory authority will be sought before CCTV images are disclosed.

## Disclosure of CCTV images is recorded in the CCTV Operating Log Book and contains:

- The name of the police officer or other relevant person in the case of other agencies/bodies receiving the copy of the recording;
- Brief details of the images captured by the CCTV to be used in evidence
- or for other purposes permitted by this policy;
- The crime reference number where relevant; and
- Date and time the images were handed over to the police or other body/agency.

Requests of for CCTV images for staff disciplinary purposes (or complaints purposes) must be authorised by HR or a director.
Requests for CCTV information under the Freedom of Information Act 2000 will be considered in accordance with that regime.

## Complaints Procedure

Any complaints relating to the CCTV system should be directed in writing to the directors and in any event within 7 days of the date of the incident giving rise to the complaint. A complaint will be responded to within a month following the date of its receipt. Records of all complaints and any follow-up action will be maintained by the company.

# EQUIPMENT POLICY

## Introduction

The company may issue a laptop, desktop computers, mobile phone, access cards, other equipment and accessories to certain users to facilitate the company's business needs. Users shall exercise appropriate professional judgment and common sense when using company's computers, equipment and accessories.

All computers, equipment and accessories are company property and are provided to company users for a period of time as deemed appropriate by the company. As a condition of their use of company's computers, users must comply with and agree to all of the following:

- Prior to being issued company IT equipment, Users will sign the Information Security Policy.
- Users should NOT attempt to install software or hardware or change the system configuration including network settings.
- Users are expected to protect laptops, equipment and accessories from damage and theft.
- Each user is monetarily responsible for any hardware damage that occurs off Q3 premises and/or software damage (including labour costs).
- Users will not be held responsible for computer problems resulting from regular work-related use; however, users will be held personally responsible for any problems caused by their negligence as deemed by Q3.
- Users will provide access to any laptop computer, equipment or accessories they have been assigned upon Q3's request.

## General Rules

You are responsible for protecting your equipment from loss or theft and for protecting the information it contains. These rules are provided to assist in assuring that your laptop is always secure. All conceivable situations cannot be covered in this document. Users must realise that common sense should be your guide when faced with unusual or unforeseen situations.

- Power off your laptop whenever it is not in use. Do not carry the laptop in suspend or hibernation mode.
- Use laptop lock-down cable systems whenever possible.
- Personal use of the company computers, equipment and accessories is prohibited
- Keep your laptop close to you and in sight. Otherwise, keep it locked away securely. It only takes a moment for a thief to walk away with your laptop.
- Never store passwords with your laptop or in its carrying case.
- Other forms of user authentication should always be kept separate from your laptop.
- Travel without your laptop if it is not needed.
- Do not place drinks or food near your laptop.

## While at the Office

- When away from your workspace, leave your laptop in locked / "log in required" lock screen status.
- Laptops should be taken home at night or secured out of sight in a locked drawer, cabinet, or locked compartment of your desk.
- Do not leave your laptop unattended if you leave the meeting room. Ensure that someone is designated to remain in the room with any laptops, or that the meeting room door is locked.

### While Traveling in a Car

- Extreme temperatures can damage a laptop. You should not leave a laptop in an unattended vehicle.
- If you must leave your laptop in an unattended vehicle for a short period of time, always lock your laptop in the boot of the car. A visible laptop is a target. This should also apply to your daily commute, as you never know when you may decide to make a “quick stop” for a break.
- On rare occasions when a vehicle may not have a boot or lockable compartment, the laptop must still be locked in the vehicle and stored out of sight.

### In Hotels

- Never leave your laptop unattended in hotel rooms.
- If you leave your room for any period of time, secure your laptop in the room safe. If a room safe is too small or unavailable, lock your laptop in your travel luggage.
- Always attempt to keep evidence that you may be traveling with a laptop out of site.
- Store the carry case and peripherals, such as a mouse and a charger, in your travel luggage.

### Risks/Liabilities/Disclaimers

All terms and conditions as stated in this document are applicable to all users of Q3 Equipment & Sites. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures herein. Any user violating these policies is subject to disciplinary actions deemed appropriate by Q3.

# BRING YOUR OWN EQUIPMENT POLICY (BYOD)

## Introduction

Devices, such as smartphones, tablet & computers, are important tools for the organisation and their use is supported to achieve business goals. However, these devices (personal or company owned) also represent a significant risk to company information security and data protection. If the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organisation's data and IT infrastructure. This can subsequently lead to costly data leakages and system infection.

We have developed this policy to protect our information assets in order to safeguard our customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of all devices when accessing the corporate or other networks network and is intended to protect the security and integrity of our data and technology infrastructure. The company reserves the right to restrict the use of devices if users do not abide by the policies and procedures outlined below.

## Scope

All mobile devices, owned by users, are expressly prohibited from accessing and or connecting to the company 'corporate' network, data and systems. This includes smartphones, tablets and computers.

- Exceptions to the policy may occur where there is a business need; however, a risk assessment must be conducted by management and written approval provided in advance.
- Users connecting to any company provided network must agree to the terms and conditions set forth in this policy and is subject to all company Information Security policy's
- The company has a zero-tolerance policy for texting or emailing while driving and only hands-free talking and calling while driving is permitted.
- In order to prevent unauthorized access, mobile devices must be password protected using the features of the device.
- The mobile device must lock itself with a password or PIN if it is idle for five minutes.
- Rooted (Android) or jailbroken (iOS) mobile devices are strictly forbidden from being connected to the company network.
- Users may not use corporate workstations to backup or synchronise mobile device content such as media.

## Risks/Liabilities/Disclaimers

It may be possible for a non-corporate owned device to connect to corporate services if a device connects to such a service provided by the company the company may:

- Remote wipe a device, all data and or company data on the mobile device will be lost, including personal data. Including personal email, photos, contacts, photographs, media files, etc.
- The company reserves the right to disconnect mobile devices or disable services without notification.
- Any removable media may be encrypted or deleted.

# INTERNET, EMAIL AND SOCIAL MEDIA USAGE POLICY AND GUIDELINES

## Introduction

This policy sets out the obligations and expectations on employees of [Company] including contractors and temporary staff, who use the Company's IT facilities. These facilities are provided to assist with day to day work. It is important that they are used responsibly, are not abused, and that individuals understand the legal, professional and ethical obligations that apply to them.

## Authorisation

No person is allowed to use Company IT facilities who has not previously been authorised to do so by the Company IT Department or their Line Manager. Unauthorised access to IT facilities is prohibited and may result in either disciplinary action or criminal prosecution.

## Legislation

All users shall comply with all current relevant legislation. This includes (but may not be restricted to) the following:

## Data Protection Act 1998 / the General Data Protection Regulations (GDPR)

Any personal information on an individual which the Company holds is covered by this legislation. This includes emails too. If you receive a subject access request you should refer this immediately to your line manager.

Users need to be sure that they are not breaching any data protection rules when they store or use information and when they write and send emails. This could include but is not limited to:

- Using data which has not been kept up-to-date.
- Passing on or processing personal information about an individual without their consent.
- Keeping personal information longer than necessary.
- Sending personal information outside the country.

If any breach of data protection rules is discovered such as the leaking or hacking of personal or sensitive data, this should be reported immediately to your line manager, and any immediate action should be taken to close down such leaks. Your line manager will ensure this is properly investigated and the appropriate reporting actions taken if necessary.

## Computer Misuse Act 1990

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

## Copyright Design and Patents Act 1988

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

## Defamation Act 1996

Under this Act it is an offence to publish untrue statements which adversely affect the reputation of a person or group of persons.

## Terrorism Act 2006

This Act has makes it a criminal offence to encourage terrorism and/or disseminate terrorist publications.

### Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

This allows for any organisation to monitor or record communications (telephone, internet, email, and fax) for defined business-related purposes.

### Responsibilities

All Users are expected to act in a manner that will not cause damage to IT facilities or disrupt IT services. Any accidental damage or disruption must be reported to the IT department or your line manager as soon as possible after the incident has occurred. Users are responsible for any IT activity which is initiated under their username.

### Use of the Internet

Use of the Internet by employees is encouraged where such use is consistent with their work and with the goals and objectives of Q3 in mind. Reasonable personal use is permissible subject to the following:

- Users must not participate in any online activities that are likely to bring Q3 into disrepute, create or transmit material that might be defamatory or incur liability on the part of the Company, or adversely impact on the reputation of the Company.
- Users must not visit, view or download any material from an internet site which contains illegal or inappropriate material. This includes, but is not limited to, pornography (including child pornography), obscene matter, race hate material, violence condoning messages, criminal skills, terrorism, cults, gambling and illegal drugs.
- Users must not knowingly introduce any form of computer virus into the Company's computer network.
- Personal use of the internet must not cause an increase for significant resource demand, e.g. storage, capacity, speed or degrade system performance.
- Users must not "hack into" unauthorised areas.
- Users must not download commercial software or any copyrighted materials belonging to third parties, unless such downloads are covered or permitted under a commercial agreement or other such licence and approved by the Company.
- Users must not use the internet for personal financial gain.
- Users must not use the Internet for illegal or criminal activities, such as, but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal drugs.
- Users must not use the internet to send offensive or harassing material to other users.
- Use of the internet for personal reasons (e.g. online banking, shopping, information surfing) must be limited, reasonable and done only during non-work time such as lunch-time.
- Use of gambling sites, online auction sites and other such inappropriate websites is **not** permissible. If you are in any doubt, you should confirm with your line manager whether a site is permissible or not before accessing the site.
- Staff may face disciplinary action or other sanctions (see below) if they breach this policy.

### Use of Email / Instant messaging

Messages sent or received on the Company email / IM system form part of the official records of Q3 they are not private property. The Company does not recognise any right of employees to impose restrictions on disclosure of such messages within the Company. These may be disclosed through legal obligations, as part of legal proceedings (e.g. tribunals), and as part of disciplinary proceedings. Users are responsible for all actions relating to their IT account including username and password, and should therefore make every effort to ensure no other person has access to their account.

When using Company email / messaging systems, users must:

- ensure they do not disrupt the Company's wider IT systems or cause an increase for significant resource demand in storage, capacity, speed or system performance e.g. by sending large attachment to a large number of internal recipients.
- ensure they do not harm the Company's reputation, bring it into disrepute, incur liability on the part of the Company, or adversely impact on its image.
- not seek to gain access to restricted areas of the network or other "hacking activities"; this is strictly forbidden.
- not use the system for the creation, retention or distribution of disruptive or offensive messages, images, materials or software that include offensive or abusive comments about ethnicity or nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs or social background. Employees who receive emails / messages with this content from other employees of the Company should report the matter to their line manager or supervisor.
- not send emails / messages that might reasonably be considered by recipients to be bullying, harassing, abusive, malicious, discriminatory, defamatory, and libellous or contain illegal or offensive material, or foul language.
- not upload, download, use, retain, distribute, or disseminate any images, text, materials, or software which might reasonably be considered indecent, obscene, pornographic, or illegal.
- not engage in any activity that is likely to
    - Corrupt or destroy other users' data or disrupt the work of other users
    - Waste staff effort or Company resources, or engage in activities that serve to deny service to other users
    - Be outside of the scope of normal work-related duties – for example, unauthorised selling/advertising of goods and services
    - Affect or have the potential to affect the performance of damage or overload the Company system, network, and/or external communications in any way
    - Be a breach of copyright or license provision with respect to both programs and data, including intellectual property rights
- not send chain letters or joke emails from a Company account.

Staff who receive improper email from individuals inside or outside the Company, should discuss the matter in the first instance with their line manager or supervisor.

Personal use of a Q3 email / message account is **not** permitted.

### Email Good Practice

The Company has good practice guidelines for dealing with email when staff are out of the office for longer than three days. When activating the "out of office" facility messages should name an alternative member of staff for correspondents to contact if necessary. This will ensure that any important messages are picked up and dealt with within required timescales.

During periods of absence when highly important emails are anticipated, the employee (or manager) should make arrangements for notification and access by another appropriate member of staff.

Where sensitive and confidential information needs to be sent via email for practical reasons, please be aware that email is essentially a non-confidential means of communication. Emails can easily be

forwarded or archived without the original sender's knowledge. They may be read by persons other than those they are intended for.

Users must exercise due care when writing emails to avoid being rude or unnecessarily terse. Emails sent from the Company may be interpreted by others as Company statements. Users are responsible for ensuring that their content and tone is appropriate. Emails often need to be as formal and business-like as other forms of written correspondence.

Users should delete all unsolicited junk mail, and in the process of archiving emails, users should ensure inappropriate material is not archived.

The Company provides a current and up to date automatic virus checker on all networked computers. However, caution should be used when opening any attachments or emails from unknown senders. Users must best endeavour to ensure that any file downloaded from the internet is done so from a reliable source. It is a disciplinary offence to disable the virus checker. Any concerns about external emails, including files containing attachments, should be discussed with the IT / Line Manager.

### Use of Social Media

Many Q3 employees will already be using social media in their personal lives. When you are not at work, it is, of course, entirely up to you to decide whether and how you choose to create or participate in a social media space or any other form of online publishing or discussion. This is your own business. The views and opinions you express are your own.

However, if you identify yourself as an employee of the Company or as being associated with it in any way, you must be mindful of this when participating in social media. We have a responsibility to make you aware that, even where you don't intend it, you can harm the company's business and reputation when using social media in a personal capacity, and that breaching this policy outside of work can still result in disciplinary action.

### Legitimate Access to Prohibited Material

There may be circumstances where users feel that the nature of their work means that they are required to access or use material prohibited under this policy. If so, this should be discussed with the Line Manager concerned. The Company is legally responsible for the content and nature of all materials stored on/accessed from its network.

### Remote Users

Users may sometimes need to use Company equipment and access the Company network while working remotely, whether from home or while travelling. The standards set out in this document apply to Company employees whether or not Company equipment and resources are being used.

### Monitoring

All resources of Q3 including computers, tablets, phones, external drives, USB drives, email, voicemail etc. are provided for legitimate use. If there are occasions where it is deemed necessary to examine data beyond that of the normal business activity of the Company then, at any time and without prior notice, the Company maintains the right to scrutinise any systems and inspect and review all data recorded in those systems. This will be undertaken by authorised staff only. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists in the management of information systems.

### Penalties for Improper Use

*Withdrawal of facilities*

1. Users in breach of these regulations may have access to Company IT facilities restricted or withdrawn.

*Disciplinary Action*

2. Breaches of these regulations may be dealt with under the Company's disciplinary procedures. It may lead to termination of employment from the Company.

*Breaches of the law*

Where appropriate, breaches of the law will be reported to the police.

## MESSAGING POLICY

### Introduction

Messaging consists of any message distributed by electronic means from and or to one or more recipients via a network. This includes email and Instant messaging.

Instant messaging technology is a type of online chat allowing text transmission over the Internet or another computer network. Messages are typically transmitted between two or more parties, when each user inputs text and triggers a transmission to the recipient(s), who are all connected on a common network.

It differs from email in that conversations over instant messaging happen in real-time (hence "instant"). Most modern instant messaging applications (sometimes called "social messengers", "messaging apps" or "chat apps") use push technology and add other features such as emojis (or graphical smileys), file transfer, chatbots, voice over IP, or video chat capabilities.

Instant messaging applications can store messages with either local-based device storage (e.g WhatsApp, Viber, Line, WeChat, Signal etc.) or cloud-based server storage (e.g Telegram, Skype, Facebook Messenger, Google Hangouts, Discord, Slack etc.).

To effectively safeguard users, company data and the collection, storage and or usage of personal data and the implications or breaching Global Data Protection Regulations this policy ensures that we engage and use the correct technology to enable effective communication and collaboration throughout our businesses.

The companies only approved collaboration tools approved for messaging is Microsoft Teams and Microsoft Outlook accessed through a company authorised account.
All other messaging platforms are expressly prohibited from use for communication of company business.

### Policy Scope

This policy applies to all staff, contractors and volunteers at the company who use messaging services — no matter whether for business or personal reasons.

It applies no matter whether that messaging takes place.

Messaging services include but are not limited to:
- Microsoft Teams
- WhatsApp
- Facebook messenger
- Snapchat
- SMS

## Responsibilities

Everyone who operates a messaging account or who uses their personal accounts at work has responsibility for implementing this policy. However, these people have key responsibilities:

1. The directors are ultimately responsible for ensuring that the company uses messaging safely, appropriately and in line with the company's objectives.
2. The directors are responsible for providing apps and tools to manage the company's messaging capability and track any key performance indicators. They are also responsible for proactively monitoring for security threats.
3. The directors are responsible for assessing any exceptions and the risk they may pose to the company on a case-by-case bases and will be formally documented and reviewed.

## Basic advice

Regardless of which messaging platforms (including email) you are using or whether they're using business or personal accounts please follow these simple rules helps avoid the most common pitfalls.

Do not send commercially sensitive information, data that business often class as commercially sensitive such as:

- Access codes
- Financial information
- Operational data
- Pending merges & acquisitions
- Cost information
- Environmental measures
- work obligations
- identity of shareholders and or officials
- employee information

Do not send personally identifiable information, data used to confirm an individual's identity such as:

- Full name
- National Insurance Number (NI)
- Driver's license
- Mailing address
- Credit card information

- Passport information
- Financial information
- Medical records
- Data should be deleted if no longer needed for its stated purpose, and personal information should not be shared with sources that cannot guarantee its protection.
- Establish consent to process the data

### Authorised users

Only people who have been given access and authorised to use the company's authorised messaging platforms may do so.

### Authorised messaging platforms

The use of the following platforms and services is approved by Authorised users

- Microsoft Teams
- Microsoft Outlook

The use of all other messaging platforms is expressly prohibited without the consent of a company director.

### Creating and using messaging

Messaging accounts, groups, rooms, direct messages, channels or any other medium in the company's name must not be created unless approved by a director.

If there is a case to be made for use of an alternative messaging platform, users should raise this with a company director.

### Further information & specifics

WhatsApp has taken steps to pass liability to users, rather than the app itself, and the 'WhatsApp GDPR policy', states that non-personal use is against the terms of service. Therefore liability passes to the company if it uses WhatsApp.

This put the responsibility on the company to assess how we use the app with regards to customers & staff. As individual consent and controls are required by the company. The company has taken the decision not to use WhatApp or sanction the use of WhatsApp in any way.

Whilst we advise against the use of WhatApp for the forementioned reasons we are aware some customers may wish to communicate with us via WhatsApp. If this is unavoidable a director will assess the risk and may implement the correct controls with management teams to establish consent and the appropriate controls to process data on WhatsApp.

### Risks/Liabilities/Disclaimers

Knowingly breaching this messaging policy is a serious matter. Users who do so will be subject to disciplinary action, up to and including termination of employment.

Users may also be held personally liable for violating this policy.

Where appropriate, the company will involve the police or other law enforcement agencies in relation to breaches of this policy.

# REMOVABLE MEDIA POLICY

## Introduction
Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organisations.

## Purpose
The purpose of this policy is to minimise the risk of loss or exposure of sensitive information maintained by Q3 and to reduce the risk of acquiring malware infections on computers and systems.

## Scope
This policy covers all removable media that contains company data or that is connected to a Q3 network.

## Policy
Q3 users may not use removable media in their work computers unless it is encrypted.

Sensitive information should be stored on removable media only when required in the performance of assigned duties or when responding to legitimate requests for information and must be pre-authorised by a company director.

When sensitive information is stored on removable media, it must be encrypted in accordance with the company's Encryption Policy. Exceptions to this policy may be requested on a case-by-case basis by raising an IT Security Exception Request.

## Definitions
### Removable Media
Removable media is defined as devices or media that is readable and/or writable by the end user and can be moved from computer to computer or other hardware capable of reading the data without modification.

This includes flash memory devices such as USB drives, SD cards, cameras, MP3 players and Mobile devices such as, Mobile Phones, Tablets & PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and software disks.

## Encryption
Encryption is a procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process. Removable media is subject to the Q3 Encryption Policy.

## Malware
Malware is defined as software of malicious intent/impact such as viruses, worms, and spyware.
Company Network

Being connected to a company network includes the following:

- If you have a network capable device (e.g. laptop) plugged into a Company occupied and or owned building, then you are connected to the corporate LAN (local area network).
- If you have a wireless capable device (ex. laptop, iPhone) and connect to any Q3 Wireless network, then you are connected to the WLAN (wireless local area network).

- If you connect from a computer through the company VPN (virtual private network), you are then connected to the company LAN (local area network).
- If you are connected to company resources via the internet such as cloud services, you are the connected to the company cloud network.

## Sensitive Information

Sensitive information is defined as information which, if made available to unauthorised persons, may adversely affect the company, its products, or services and customers served by its activities.

Examples include, but are not limited to, personal data and financial information & intellectual property.

## Risks/Liabilities/Disclaimers

Anyone found to have violated this policy may be subject to disciplinary action, up to and including investigation, suspension of access to technology resources or termination of employment.

A breach of this policy by a temporary worker, contractor or supplier may result in action up to and including termination of their contract.

# ENCRYPTION POLICY

## Introduction

The purpose of this document is to provide guidance to all Q3 users on the use of encryption, and to ensure Q3 and Personal Identifiable Information (PII) always remains secure and confidential.

This policy is designed to protect Q3 as an organisation, and users by defining the use and application of encryption technology when accessing, storing and transmitting (processing) Q3 corporate, personal or other data.

The Encryption Policy shall be used to enable Q3 IT systems and media, from unauthorised access through use of an approved encryption solution where it has been decided as being required
All Q3 users are required to comply or abide by the terms of this policy.

## Scope

This policy applies to those members of staff that are directly employed by Q3 and for whom Q3 has legal responsibility, as well as any Processors/contractors/sub-contractors/third parties processing Q3 data or accessing Q3, or anyone authorised to undertake work on behalf of Q3. For those staff covered by a letter of authority/honorary contract or work experience, the organisation's policies are also applicable whilst undertaking duties for or on behalf of Q3.

From this point forward these staff will be referred to as users and include any previous definition of ('users') within this document.

## Principles

To summarise, all Q3 data will be encrypted at rest, for example, on desktops, laptops, portable devices, such as CDs and memory sticks, and in transit.

Q3 will require approved encryption software to be installed on information system devices. Users shall not bypass, cause to bypass or use any tools or software to bypass the encryption software installed on devices by Q3. In addition, users are strictly prohibited from downloading, installing or using their own or other encryption software.

All users who work for Q3 have the ability to remotely access Q3 information systems and information and must do so through an encrypted connection.

All wireless connections must be encrypted to current approved standards. Current approved standards will be subject to an ongoing evaluation in line with national standards or requirements
All IT service provider(s) for Q3, must:

- use encryption software that has been approved.
- apply encryption to servers, non-console administrative access and remote access

***(where applicable);***
apply file integrity monitoring software to alert personnel to any modification of critical systems or content files; and have fully documented Key Management Procedures in place that include, but are not limited to, the following:

- generation of strong keys;
- secure key storage and distribution;

- periodic key changes and destruction of old keys;
- split knowledge and dual control;

replacement of known or suspected compromised keys; and revocation of old or invalid keys.

### Laptops and Tablets

All laptops and tablets shall be protected by a full disk encryption solution approved to protect the identified security classification.

If a full disk encryption solution has not been, or cannot be, configured on the device then the risks to the information shall be assessed and either:

- An alternative encryption solution shall be utilised for which the risks have been accepted by the Business Solutions team; or
- The device remains unencrypted and the risks shall be qualified and accepted by the submission of a 'Security Exception' which is approved by the Business Solutions Team; this will mean that only publicly available information can be processed on the device.

### Removable Media

All removable media shall be encrypted, or individual files/directories copied to the removable media shall be encrypted with an appropriate encryption solution approved to protect the security classification of the information on the media.

If it is not possible or practical to encrypt the removal media or individual files/directories, then an assessment of the potential risks to the information shall be made. The Operations director shall determine what security measures need to be put in place a 'Security Exception' raised and whether the removable media can be used to store the information.

### Email

All email with sensitive or PII shall be the user's responsibility to ensure such data is encrypted before the email is sent.

If it is not possible or practical to use the secure networks then the proposed content of the email shall be assessed by the user, with advice from the directors, and if personal or confidential data is included within the e-mail, it should not be sent.

### Encryption Solutions

The directors shall approve all encryption solutions.

Preference shall be given to encryption products approved for use by the Government and Public Sector that are listed on the NCSC website.