Acceptable Use of IT and Remote Working Policy

Table of Contents

Document Control

Document Control	
Title:	Acceptable Use of IT and Remote Working Policy
Reference:	IS-POL-001
Version:	0.1
Date:	27.01.2023
Status:	Final
Owner:	Product Director
Classification:	Internal

1 Purpose

Protecting our business is a responsibility we all share and requires the right balance in giving our people the freedom to succeed whilst enforcing guidelines and policies that ensure that we work safely, securely and responsibly.

This policy sets out how we manage and handle our IT equipment and data, and the standards that must be observed when using and/or accessing them.

The misuse of Triangle's IT equipment and data can seriously damage Triangle's business and reputation, and therefore it is extremely important that all staff, including employees, contractors and relevant third parties, read and understand the policy – as the responsibilities outlined must be followed in full.

Breaches of this policy may be dealt with under the Disciplinary Policy and, in serious cases, could be treated as gross misconduct leading to summary dismissal.

2 Introduction to the Policy

Triangle's data is essential to the current and future success of the business. Maintaining the security and availability of Triangle's data is a necessity and is core to our business.

We are required to ensure that Triangle data is not at risk through loss or unauthorised modification (whether deliberate or inadvertent) and that the integrity of our data is maintained throughout its lifecycle.

Triangle has legal, statutory, regulatory and contractual obligations that include information security. Furthermore, we need to demonstrate information security to our customers. Triangle's information security policies, standards and procedures assist us in achieving these goals. You have an obligation to adhere to these policies, standards and procedures.

Information security is the preservation of the confidentiality, integrity and availability of information:

- Confidentiality – Protecting sensitive or personal information from unauthorised disclosure, both to outsiders, and to employees or contractors who have no requirement to access such information in the course of their duties;
- Integrity – Safeguarding the accuracy and completeness of information and information processing methods, against any unauthorised changes;
- Availability – Ensuring that information and associated services are available to meet Triangle's business needs.

Information security is required during the whole lifecycle of information based in Triangle, from the moment it is collected or created, throughout its usage, to ultimate disposal. Appropriate measures need to be applied to ensure that information security is maintained. Information security promotes trust and confidence in Triangle's services, business practices and IT infrastructure and systems.

The achievement of information security requires a combination of policies, standards, procedures, appropriate organisational structure, physical security considerations, and measures to safeguard the IT network infrastructure and information systems.

If you need assistance on any of the information security requirements contained in this policy, you should seek advice from your line manager or from Information Security.

3 Scope

This policy applies to all Triangle personnel irrespective of status, including temporary staff, contractors, consultants and third parties who have access to Triangle's core data and systems.

It applies to personnel using devices purchased by Triangle, or devices approved by Triangle for the purposes of accessing Triangle's core data and systems (see detail in policy for clarity.) It applies to all devices,

For the avoidance of doubt, Triangle's core data and systems means anyone with access to Triangle data in Salesforce, Xero or Dropbox, or who has a Triangle email address. It does not mean third parties who only have

access to 'public' information via limited Dropbox shared folders, or who are covered by other equivalent contractual arrangements (for example, QES Ltd for the Outcomes Star Online).

It applies whether the access to and use of systems and data occurs on Triangle's premises or remotely from any location including, but not limited to, home working.

4 Policy Statement

Triangle's policy is that our facilities, equipment, systems and data shall only be used and accessed in acceptable ways that ensure the confidentiality, integrity and availability of the information.

5 Roles and Responsibilities

- The Product Director is responsible for this policy and shall ensure that this policy is up-to-date and relevant.
- Operational teams shall manage the implementation of any specific requirements detailed in this policy for in house and third party applications, systems and services.
- Development teams shall ensure that the methods and capabilities as detailed in the policies and standards are detailed as use cases and appropriate capabilities are created within Triangle's own applications, systems and services to ensure the policies can be applied.
- Line managers are directly responsible for implementing this policy within their functions/departments, and for adherence by their staff.
- All Triangle staff shall comply with this policy and facilitate its implementation.

6 What Is Your Responsibility?

You are personally accountable for assisting Triangle in maintaining the confidentiality, integrity and availability of its information.

All staff are faced with information security risks and responsibilities daily. Effective security management is about mitigating our risks. From an organisational perspective, this has been achieved through the development of information security policies, standards and procedures, together with complementary information security training and awareness.

Poor information security management can, for example, lead to:

- Leakage and compromise of sensitive information, e.g. personal or commercial information;
- Loss of critical information;
- Fraudulent activities, e.g. identity theft; and
- Failure to comply with legal, statutory, regulatory or contractual requirements.

A direct result of such an occurrence could be that our business, research opportunities and relationships with our customers will suffer. In order to avoid such instances, we shall all take necessary steps to ensure that security is maintained, including the following:

- Obtain advice from line managers, or the Information Security team when unsure;
- Request training when needed;
- Complete training when required;
- Report any suspected security incidents as directed by Triangle; and
- Make recommendations on how we can improve our information security.

Enabling Triangle to operate in a secure environment requires us all to work as a team towards the same goal of information security.

7 Acceptable Use of Triangle-owned IT Assets

For members of staff who will be accessing Triangle's core data and systems, all IT processing facilities and equipment to be used in connection with Triangle's information shall be formally configured and authorised by the Managed IT Support Provider (It's What's Next CIC).

The Managed IT Support Provider shall manage an inventory of all acquired IT assets. This includes recording of personnel authorised to use the IT assets, and any labelling requirements for the IT assets. All IT assets shall be returned to the business when they are no longer required – this will help maintain the IT asset inventory.

All of the IT equipment, devices and software that you have been assigned remains the property of Triangle. You have an obligation to ensure that this equipment and software is safeguarded and only used as intended by Triangle:

- You shall always take care of IT equipment allocated for your use, and treat it as if it is your own;
- You shall protect your IT equipment against theft and unauthorised access;
- You shall not store any access control device with equipment or devices which are reliant on the same device for multi-factor authentication;
- You shall not expose your IT equipment to any environmental hazard, such as extremes of temperature;
- You shall not install any unauthorised or unlicensed software on your IT equipment. If you require any software for your work, you shall get approval from your line manager or the Managed IT Support Provider;
- You shall not modify your IT equipment in any way; this includes any amendments to the hardware and software configuration;
- You shall not install any unauthorised tunnelling or peer-to-peer software or service;
- You shall not install any monitoring avoidance software or service;
- You shall always report any IT problems to the Managed IT Support Provider

Specific acceptable use requirements in connection with protection against malicious code such as viruses and spyware, secure use of e-mail and Internet access, and protection of copyright materials are documented below.

Triangle provides primary access to its systems and IT equipment for business use but recognises that there are times when you will need to complete personal tasks online, and reasonable personal use of equipment is permitted.

When you use Triangle equipment assigned to you for personal and/or business matters, you shall ensure that you do not:

- Violate any laws, professional standards or Triangle policies;
- Create the appearance of impropriety on the part of Triangle;
- Violate or infringe upon the intellectual property rights and property of others;
- Put the rights and property of Triangle or its clients at risk;
- Compromise, embarrass or bring into disrepute Triangle's brand, reputation or relationships with its clients;
- Utilise Triangle identities, including business e-mail address(es), for personal accounts or services;
- Impede any Triangle business activity, including your own productivity;
- Impersonate others or position yourself as an authorised spokesperson for Triangle in online forums or social media without prior written approval.

If you are using Triangle equipment for personal use (such as conducting online banking, booking a holiday or shopping) you do so at your own risk, and, if you have any concerns about the security of Triangle's equipment, you shall use alternative means for conducting your personal business.

8 Use of approved devices

Personnel not using Triangle-owned devices to access Triangle's core data and systems can use personally owned devices only when that device has been approved by Triangle and formal authorisation has been provided by the Managed IT Support Provider.

For a device to be approved, Triangle must have the following information and standards:

- Is the operating system Windows or macOS?
- Is the operating system version currently supported by the vendor?
- Are operating system updates set to auto-install?
- Is the version of Microsoft Office installed supported by Microsoft (if installed)?
- Are Microsoft Office updates set to auto-install (if installed)?
- Is an appropriate antivirus product active?
- Is encryption enabled on the device?

If the device cannot be approved then access to Triangle's core systems and data will be denied or revoked.

9 Information Classification and Handling

All information that is handled by Triangle has a classification to determine the level of security it requires and the way in which it shall be handled. The Information Classification and Handling section of the Information Security Policy defines the information classification scheme and applies to all information irrespective of its form, including electronic information, e.g. databases and files, computer media-based information, e.g. stored on CDs, DVDs and USB devices, and paper-based documents, e.g. contracts, facsimiles and printed reports.

For every document you produce, you are personally accountable for defining its classification on behalf of your business unit or department. When you are classifying information, you shall consider its sensitivity and how much protection it needs when being shared or stored.

When using Triangle's information, you shall handle it in a secure manner based upon its classification.

More information can be obtained from the Information Classification and Handling section of the Information Security Policy.

10 Site Security

Physical security involves protecting Triangle's premises, staff, information and IT assets from unauthorised physical access and physical security threats, e.g. fire, invasion, theft and wilful damage. All staff shall support Triangle's site security requirements. Staff shall not allow unauthorised physical access into Triangle's offices and shall report physical security threats to senior management as soon as possible using Triangle's standard reporting procedures.

If you are allocated with keys or other controls (such as electronic key fobs or swipe cards) for access to Triangle's offices or facilities, ensure you keep them in a secure location, and protected from unauthorised access. If they are lost or stolen, you shall immediately report this, in line with the Information Classification and Handling section of the Information Security Policy..

11 Removal of Property and Security of Equipment Off-Premises

All staff are responsible for protecting authorised off-site equipment against physical security threats and unauthorised access. See section 21 below for more detail.

Staff shall always ensure that off-site Triangle information is securely handled in line with the Information Classification and Handling section of the Information Security Policy..

12 Secure Disposal and Re-use of Equipment

All of Triangle's information and software shall be securely wiped from Triangle's IT equipment before disposal or re-use of the equipment. All equipment intended for disposal and re-use shall be returned to the Managed It Support Provider, who shall securely wipe Triangle's information and software from it, using established procedures.

Where data cannot be securely wiped the media shall be removed and retained in line with the Information Classification and Handling section of the Information Security Policy. or securely destroyed to ensure the information cannot be later retrieved.

13 Protection against Malware

Computer viruses, spyware, remote access Trojans, ransomware and other forms of malicious code (malware) exploit vulnerabilities in software programs and can cause loss and damage to Triangle's information, software and IT equipment or unauthorised access to Triangle systems and services.

Triangle uses a variety of products, e.g. mobile device management, monitoring, anti-virus and software security patches, network based scanning and firewalls which are frequently updated to reduce the threat from viruses and other malicious code.

You shall not change or remove these controls on your Triangle device, or an approved device, otherwise Triangle's IT network, systems and information will become more vulnerable to the threat from viruses and other malicious code.

In addition to these controls, Triangle is also dependent on its staff, who shall remain vigilant to protect Triangle from malicious code. You shall ensure that:

- You do not introduce a virus or malicious code into the corporate network, by downloading unauthorised or suspect software from the Internet or from computer media, e.g. DVDs, CDs and USB storage or smart devices onto your PC, laptop or any Triangle system or service;
- All software and data which originates from outside Triangle shall be checked for viruses and malicious software prior to it being opened or used – if you need help, contact the Service Desk;
- If you are suspicious of a virus or malicious code, you shall stop using your PC or laptop immediately and contact the Managed IT Support Provider;
- If you receive a suspicious e-mail, you shall not open or preview it, or the attachment or any hypertext link, as this may well activate a virus or other form of malicious code. Immediately contact the Managed IT Support Provider.

There may also be 'hoax' virus messages in circulation which are not actually viruses at all, but plain e-mail messages asking you to take some sort of action, such as deleting files on your computer and forwarding the message which then due to the number sent become 'viral' themselves. These messages themselves are not infected with a virus, and are spread by playing on people's fears, and fooling them into following the instructions. If you receive a message warning you of a virus, you shall immediately contact the Managed IT Support Provider.

14 Secure Handling of Media and Documentation

Care shall be taken to protect all documentation and computer media, e.g. DVDs, CDs and USB storage devices or smart devices containing sensitive and critical information, and measures shall be taken to ensure secure storage, transit, copying, reuse and disposal of computer media and documentation. All staff shall comply with the Information Classification and Handling section of the Information Security Policy..

When exchanging information within Triangle or between Triangle and other organisations, it is vital to assess the sensitivity of the information and handle it in accordance with the Information Classification and Handling section of the Information Security Policy..

The use of USB devices poses a risk to Triangle in respect of loss of data and other intellectual property, and potential introduction of malware. Triangle has facilities that allow the secure exchange of information without the use of USB drives. USB drives should not be used without the express permission and regulation of the Managed IT Support provider who will ensure the USB device is malware-scanned and encrypted.

When dealing with printed documents, always ensures that you are aware of their security classification and handling requirements. Sensitive documents shall not be left or reviewed in public or on public transport, or left unattended on desks, printers, facsimiles and other equipment where they are vulnerable to unauthorised access and theft.

You shall always lock sensitive computer media and documents away when left unattended.

15 Storage of Information in the Cloud

Users shall only store or share Triangle information in the Cloud using products and services approved by Triangle.

16 E-mail Security and Secure Internet Access

E-mail and Internet are provided to you as a means of improving your communications, collaboration, knowledge and effectiveness at work. Triangle's e-mail and Internet facilities are intended for business use. All usage of Triangle's e-mail and Internet facilities is treated as the property of Triangle and shall not be regarded as private.

Triangle e-mail may not be used for exchange of inappropriate (including pornographic, obscene, offensive, racist, defamatory, harassing or intimidating) content, to facilitate personal financial gain, or for political purposes.

E-mail access shall only be made via accounts and passwords provided by Triangle. Each user shall be allocated a unique e-mail account, which shall not be shared with anyone else. Account passwords shall not be disclosed to anyone. In exceptional cases where there is business benefit, a shared e-mail account may be authorised to receive e-mails into Triangle and available to individuals through their standard e-mail access, but shall not be able to send e-mails on behalf of the shared mailbox unless specifically approved. The management of shared e-mail accounts shall be the responsibility of the relevant line manager.

Triangle's information that needs to be shared shall not be stored in individual e-mail accounts; rather it shall be stored in approved shared directories or third party applications/storage, with access controls that restrict access to only authorised users. This shall enable authorised managers and colleagues to access important information in the absence of users.

The use of personal Internet e-mail accounts for Triangle correspondence (e.g. Hotmail, Gmail and Yahoo), Internet e-mail subscription groups, peer-to-peer and instant messaging (e.g. Skype, LinkedIn, WhatsApp and Facebook) is prohibited, unless authorised for a specific and approved business purpose by the Board and the relevant line manager.

Use by Triangle staff of third party or partner e-mail accounts is prohibited for any Triangle data other than that classified as Public. Where the third party or partner requires sensitive data to be shared only approved sensitive data methods shall be used. Triangle e-mail may not be auto-forwarded to a third party or public e-mail system unless there is an approved documented business need.

Staff shall be aware that Triangle reserves the right to use monitoring tools to enforce Triangle policies, retain information from and about e-mails exchanged, and will produce periodic reports detailing use of all e-mail and Internet access facilities.

Use of e-mail and Internet access introduces security threats such as malicious code attacks, e.g. viruses, unsolicited or undesirable e-mails, attempt to initiate financial transactions, fraudulent attempts to acquire sensitive information such as research, passwords and payment card details, unauthorised content, and breaches of legislation, e.g. computer misuse and copyright legislation. If you accidentally access any material which is not permitted, you shall report this to your line manager and the Managed IT Support Provider immediately.

E-mail is an insecure method of communication and messages may well be read by those who have no authority to do so. Before sending information via e-mail, you shall first assess the handling requirements of that information as established in the Information Classification and Handling section of the Information Security Policy.and if e-mail is the correct means to exchange data.

17 Information Security in Conversations and with the Use of Telephones, Facsimiles and Recording Equipment

Due care shall be taken when using telephones, voicemail, conferencing, answering machines, facsimiles and recording equipment (e.g. photographic, video and audio equipment) to ensure the protection of sensitive information. Staff shall comply with the Information Classification and Handling section of the Information Security Policy.and the Data Protection Policy.

18 User Identification, Access and Monitoring

You shall only access and use Triangle's IT network, systems and applications if you are authorised to do so. If you are granted access, it is so that you are able to perform your duties efficiently.

You shall remember that access has been granted for your sole use by means of a unique user account and password. This applies to the different user accounts that may be granted to you for access to Triangle's network, information systems and applications. You shall not give details of your user account and password to anyone, including your line manager; you shall not share any user account allocated to you with anyone else. Triangle (within its legal rights) is able to track the activities of each user via their user account, and identify exactly what information and systems or services they have accessed and what actions have been taken. If it is your user account that is logged as attempting an unauthorised or illegal action, you may be held responsible. It is in your interests to ensure that you safeguard your user account and password details at all times.

In order the ensure compliance with legislation, regulations, contracts and its information security policies, Triangle reserves the right to monitor user activities and data flows.

19 Password Security

Passwords are a key control to maintain information security. They help us ensure that only authorised persons have access to Triangle's IT network and systems. In order for your password to be effective and remain secure, you shall comply with the following simple rules.

Ensure that your password is memorable, so that you do not need to write it down or electronically store it. Written down passwords are strongly discouraged. Electronically stored passwords are strongly discouraged, unless the passwords are secured via an IT solution that is approved by the IT Department and the Information Security Manager. Online text or documents for passwords shall never be used.

Ensure that your password is difficult for others to guess. Do not use a variation of Triangle, Outcomes Star or your name. When creating your password, you shall always use good password practice:

- DO:
    - Follow the password complexity rules prescribed in the Access Control Policy. These rules prescribe a minimum password length and the use of different types of characters;
    - When using smart devices, ensure any PIN or shape drawn/tapped is not obvious, (e.g.: square, single right angle, etc.).
- DON'T (individually or as a combination of):
    - Use your user ID;
    - Use names (e.g. your name, or the names of your partner, children and heroes, or place names);
    - Use information which is well known to others, or could be gleamed through social media (e.g.: hobbies, brands, holiday resort destinations, family/pet names, celebrities);
    - Use dates (e.g. birthdays, anniversaries, other memorable, recurring or dates associated with significant/major events);
    - Use words that people can associate you with (e.g. birthplace, home address, Triangle's address, sporting team(s));
    - Use words from any dictionary (e.g.: local and any second languages you may use);
    - Use successive passwords that follow an easily predictable pattern (e.g.: [Password]01, [Password]02, [Password]A, [Password]B);

- Use the ‘Save/Remember Password’ feature that is provided in some applications.

Ensure that you are not overlooked when typing your password. If your password is disclosed to anyone or compromised in any way, you shall change your password immediately. Regardless, you shall change your password at regular intervals, and not use previously used passwords.

20 Clear Desk and Clear Screen

Measures shall be taken to adequately protect against unauthorised physical access to Triangle’s information hosted on PCs, laptops, handheld devices (e.g. tablets, mobile telephones, and digital cameras), computer media (e.g. DVDs, CDs and USB storage devices), and paper documentation. Staff shall adhere to the Information Classification and Handling section of the Information Security Policy..

All staff shall ensure that access to their user accounts is password protected when their computer devices are left unattended, even for a small amount of time, e.g. 1 minute. This can be done by following these simple steps:

- Press Ctrl, Alt, Delete buttons together;
- A dialog box will appear. Within this, click on the ‘Lock This Computer’ option;
- Alternatively, press the ‘Windows’ button and ‘L’.

All staff shall ensure that all mobile equipment, e.g. laptops and tablets, sensitive computer media and sensitive documentation are not left unattended and insecure, but are appropriately stored in locked areas or facilities, e.g. locked cabinets, and that access to relevant keys is controlled.

At the end of a working day, you shall:

- Logoff from and shut down your PC or laptop;
- If you are a user of a laptop or handheld device, and you are not taking it with you, you shall lock it away in a drawer or cabinet with suitably restricted access.

21 Remote Working

Remote workers include:

- Mobile workers: all users who use Triangle’s information and information processing facilities whilst not located on Triangle’s premises, e.g. workers who are located in other organisations’ offices, in hotels and conferences, and travelling workers.
- Home workers: users who have been authorised to use Triangle’s information and information processing facilities whilst based at home, or larger groups of Triangle employees required to work from home during exceptional periods of disruption or mandatory changes to working practices..

Laptops, mobile phones, tablets, and other such portable equipment are expensive and valuable assets that are highly desirable, particularly to the opportunist thief. Loss of such equipment not only has an obvious financial implication, but may also compromise the information that is on the equipment itself. Exposure of this information could result in breaches of Triangle’s legal, regulatory, statutory and contractual obligations, and damage to Triangle’s reputation. For example, the loss of a laptop which holds a file containing personal details of employees is likely to result in contravention of data protection legislation. This could lead to Triangle, and possibly the individual concerned, facing a fine or in extreme circumstances imprisonment.

All policies and procedures that apply to staff based at Triangle’s offices also apply to remote workers. As your remote working environment is not fully controlled by Triangle, it is your responsibility as a mobile or home worker to ensure that appropriate security controls are implemented to protect Triangle’s information and IT assets.

Any Triangle device used at home is not provided as a replacement for a home or staff owned device and shall not be considered a family computer or device.

Physical protection of Triangle’s information and information processing facilities:

The following measures are required to reduce the risk of physical security threats to devices used for remote working and Triangle’s information.

Devices shall never be left unattended whilst unprotected, and where possible, mobile devices shall be stored within a locked cabinet, desk or room when not in use, and the associated keys shall be protected to prevent unauthorised access to the devices. Computer equipment shall not be positioned or left so that it can be easily seen through ground floor windows by members of the public.

Family members, friends, visitors or anyone else shall not use Triangle's equipment and or be given access to sensitive information.

Secure remote access to Triangle's IT network and systems:

The following measures are required to reduce the risk of security threats to information systems and networks, i.e. Triangle's information and software on computing devices used for remote working.

Triangle information should only be processed on computing devices that have been approved by the business.

All Triangle information is securely and regularly backed up to the central Triangle network systems, in order to avoid the risks of lost and out-of-date information.

22 Reporting Information Security Incidents

In order for Triangle to be able to manage and deal with information security incidents successfully, they shall be captured and logged.

If you suspect or have knowledge of an information security incident or event, or a breach of Triangle's information security policies or procedures, or a software malfunction, or a security weakness in any Triangle building, network or information system, you shall report the concern immediately, complying with the Information Security Incident Response Policy.

More information can be obtained from the Information Security Incident Response Policy.

23 Data Protection Legislation and Privacy of Personal Information

Data protection regulations, including the General Data Protection Regulation (GDPR), are concerned with the direct use of personal information, whether that information is a manual record or processed on a computer system. Data protection legislation and regulations apply to all types of personal information; this includes information which may not be thought to be confidential.

Personal data means data that relates to a living individual who can be identified from that data, or a combination of that data and other information which is in the possession of Triangle. It also includes any expression of opinion about the individual.

The GDPR has data handling principles, all of which shall be adhered to when handling personal information. The principles include specific requirements that address the security aspects of handling personal information.

If Triangle fails to abide by data protection legislation and regulations, it could be heavily fined and its business operations could be negatively impacted. Personal liability is also imposed, so if an employee is found to be contravening data protection requirements, he/she could be prosecuted too.

All staff shall comply with data protection legislation and regulations, and the Data Protection Policy. If you are unsure about any data protection requirement, contact the Data Protection Officer (DPO) for assistance. It is your responsibility to be familiar with and to adhere to the requirements of data protection legislation and regulations.

More information can be obtained from the Data Protection Policy.

24 Computer Misuse Legislation

All users shall comply with applicable computer misuse legislation. Such legislation, generally aimed at computer 'hacking', specifies offences for any unauthorised access to internal organisational systems.

Computer misuse legislation generally defines as criminal acts:

- Unauthorised access;

- Unauthorised access with intent to commit a further serious offence;
- Unauthorised modification of computer material.

Staff shall only access systems they are authorised to use. It is an offence to knowingly gain unauthorised access to a computer system, and this could result in a fine or imprisonment.

25 Policy Review Date

This policy shall be reviewed and appropriately updated on an annual basis. It shall also be reviewed and appropriately updated when there are any changes to relevant regulations on information security and/or data protection.