Capture. Share.

Group IT Policy ("the Policy")

The Vitec Group plc ("the Group")

December 2020

CONTENTS

Group IT Policy
("the Policy")

Section 1 – Purpose and confirmation statement

Scope of the Policy

The purpose of this Policy is to ensure that all employees and contractors are aware of the Group's rules with regards to:

- The use of Group supplied computer technology and services;
- The use of Group IT services accessed by third parties;
- The use of electronic communication such as email and instant messaging;
- The use of social media platforms such as Facebook, Twitter, Instagram, LinkedIn and Glassdoor, either internal or external to the Group;
- The management of personal data.

Any third parties such as visitors, agents or consultants using the Group's computer network and services are also subject to compliance with this policy. It is the **responsibility of the employee** who authorises the third party use to ensure that the third parties have read and understood the terms of this policy and agree to be bound by it. Where the policy refers to employees it is inferred that it also refers to contractors. Third party access to Group IT services may be terminated if their security and data controls are found to be inadequate.

The Policy has been implemented to protect the Group and employees' reputations and to ensure a secure, trusted, and safe computing environment for all our users. Employees deemed to be in breach of the Policy may be subject to disciplinary procedures ranging from (but not limited to) verbal warnings to instant dismissal, and may be subject to either civil or criminal penalties under the applicable legislation.

Confirmation statement

Your signature on this document indicates that you have read, understood and agree to abide by the rules set out in this Policy. In particular, you agree to the following.

- Personal use of Group's IT network and resources should be limited and reasonable and should not affect your duties.
- You shall not access websites which contain obscene, pornographic, racial, sexual, political or other material contrary to the Group's policies and values. You shall not also download, access or share such material.
- All data (including personal, confidential, or sensitive data) should be protected and carefully handled and communicated;
- You must immediately report any data security breach or threat to your line Manager, IT Department and Data Protection Lead. This includes: loss or theft of data or equipment on which data is stored; or loss of data due to unauthorised access, human error, unforeseen circumstances such as a fire or flood, or hacking attack (such as Denial of Service attack, ransomware and any other form of malware).
- You should not open work-related or private emails or attachments from your work computer which are from unknown sources as these could contain viruses which might infiltrate our network. You must be extremely wary of any email URL links or pop ups which require you to enter credentials.
- All IT equipment should be carefully secured, and laptops should be locked away at night.
- Software should not be downloaded and used without the express authorisation of IT.
  All forms of electronic communications must be conducted in a professional manner, in compliance with Vitec's Code of Conduct and the guidelines outlined in the Policy.

Group IT Policy – December 2020 version

Acceptance and Acknowledgement

Please sign and return this page to your local HR contact.

I have read and understood the terms and conditions laid out in this document and I accept the responsibilities required of me therein. I have understood that I may be required to complete an IT induction after joining the Group or undertake periodic IT training.

Failure to return this document to your local HR contact may result in your user account being locked out.

Name	
Employing Company	
Date	
Signature	

Section 2 – General Principles of IT use

Employees and contractors should be aware of the rules in using any computer service supplied by the Group.

Prohibited activities

In conjunction with the rules regarding the use of electronic communications (section 4), employees should be aware of the rules in using any computer service supplied by the Group. Employees must respect the confidentiality of information stored within the Group's systems and the integrity of the overall computing environment, ensuring that they do nothing to damage, or potentially damage, the integrity or disrupt the intended use of the systems.

The following activities are strictly prohibited:

- Attempting to gain unauthorised access to (a) any part of the Group's network or intranet or any files stored therein to which you do not have authority or permission to access and/or (b) any other computer, and employees should be aware that unauthorised access to or attempts to access a third party's computer system is a criminal offence under certain jurisdictions including the Computer Misuse Act 1990.
- The unauthorised up/downloading of and/or modification or removal of files to or on any server in the Group's network.
- Those which may disrupt the intended use of the Group's computer system or network resources.
- The unauthorised use or copying of proprietary software or copyright material (see section 3 on software use).
- Accessing or attempting to access any internet sites, or sharing of inappropriate or company sensitive material which:
    - Is obscene;
    - Contains racial, sexual, political or other hate material likely to cause offence;
    - Displays pornographic images;
    - Contains offensive language;
    - Is illegal or against the Group's policy or contrary to the Group's interest.

Personal use of the Group network and services is not strictly prohibited but it should be limited and reasonable and should not adversely affect the performance of the employee's duties. You should never use the Group network and services to access pornographic, betting, or other sites which are deemed controversial. Not only is this a violation of Vitec policy, but it also increases the risk that malware or viruses will infiltrate our network.

Personal email must be clearly marked as such either by the means of applying a category or placing into an appropriately named folder. Never use your personal email account to send a work-related email, unless there are exceptional circumstances, e.g. extended IT outage following a disaster.

Employee preventive measures

Employees should be mindful that the Group's systems contain confidential information and that unsolicited approaches may be made by third parties in an attempt to gain access to company information (also known as phishing or social engineering). Employees should be vigilant when answering the phone or replying to emails and should not divulge company or personal information unless they are certain it is to a reputable and known party. Any suspicious or unusual emails should be reported to your local IT Department. Employees responsible for making payments must never deviate from the established payments protocol. **Any supplier or customer request to change bank details held within Vitec's accounting systems**

must be confirmed in writing and independently verified by phone with a known supplier/customer contact.

IT systems and firewalls alone cannot prevent and detect the many types of external malware and virus infections. You should not open work-related or private emails or attachments from your work computer which are from unknown sources as these could contain viruses which might infiltrate our network. You must be extremely wary of any email URL links or pop ups which require you to enter credentials.

Ensure that you action all IT requests such as anti-virus software updates / password changes immediately. If you become aware or suspect that your device(s) are infected you must notify your IT Department immediately.

You must comply with the password access control rules in place within your Business Unit. “Passphrases” are deemed to be more effective; as a rule of thumb passwords should be at least 10 characters long, and have a combination of upper and lower case, numbers and characters. You have a responsibility to ensure they are changed every few months. Never share or write down a password. If you think someone knows or has used your password, change it immediately and notify your local IT helpdesk.

Rules on Bring Your Own Device (BYOD)

BYOD for work purposes is not recommended because of the implications for data integrity and IT security. Any use of personal equipment for work purposes must be expressly cleared with your IT department and the necessary protections put in place. This covers all electronic devices including but not limited to PCs, laptops, tablets and mobile phones.

Safeguarding equipment

It is the employee’s responsibility to ensure the security and integrity of any computer or communication equipment they have on loan. This includes, but is not limited to, desktop computers, laptops, modems, printers, tablets and phones.

Users of personal computers, laptops and tablet devices are also reminded that they should safeguard their systems by “locking” their desktops (with a password) when away from their desks. This applies regardless of the length of time you expect to be away from your desk. When leaving the office each day computers must be turned off and not left on stand-by overnight.

Laptops must be locked away overnight (if on Group premises), or secured with a locking system, and must be in your possession at all times when travelling. Never check-in a laptop unless required by law, and never leave a laptop in a vehicle if the vehicle is unattended.

The loss of any Group equipment should be reported to your local IT Department immediately.

Use of removable devices

Employees should be aware of the origin of such devices and should not insert an unknown device into a Group laptop or computer without it being scanned for viruses. You should contact your local IT helpdesk if you have any concerns about using devices in your possession. Only encrypted devices should be used.

Employees must not use removable data storage devices to extract Group information for their own personal use or commercial gain. Doing so would be a breach of the Code of Conduct and could lead to disciplinary action or immediate dismissal.

Use of external file sharing applications

The use of external file sharing applications for storing important information is strongly discouraged unless the use and access to the relevant external file sharing application is controlled by the IT Department. Intellectual property or personal data should never be stored in an external service that is not correctly controlled and monitored.

Protecting data

You must have a clear understanding of the nature and sensitivity of any data that is in your possession or that you have access to. This may include: confidential payroll or customer information, intellectual property such as commercial drawings, commercially sensitive information such as pricing, or credit card information, or personal data.

All files containing sensitive information, including personal information, must be password protected, and email transmission of these files should also be encrypted. For example, it is not appropriate to email payroll files without password protecting the file. Sensitive information should be shared as little as possible and where possible shared via secure links rather than emailing full attachments.

Where confidential, personal or other sensitive information is being sent by electronic communication, appropriate security measures must be used (for example password protection or encryption) to protect it. Where passwords or other security measures are used a record should be kept (in a secure manner) of passwords used or other security measures to ensure that files/documents can be accessed by other authorised users, for example, where an employee is off sick, on holiday or has left the Group.

The download of company information for personal gain is strictly forbidden and may lead to prosecution.

You must ensure that all data/information in your possession is regularly backed-up. All data should be archived in accordance with your local policy.

See section 5 regarding guidelines specific to personal data. These guidelines reflect the requirements of GDPR.

Reporting data breaches

Any actual or suspected data breach must be immediately escalated to your Line Manager, IT Department, Data Protection Lead and Group Company Secretary, who will collectively initiate further investigations, and escalation to other management at Group and Division, in accordance with the Vitec Group Information Security Incident Management Policy.

It is imperative that you report any breaches immediately so that an appropriate response can be put in place as soon as possible. For example, in the case of Phishing attacks, speed of response is absolutely critical. There may also be a legal requirement to report certain breaches to the relevant authorities within established timeframes, particularly in respect of personal data (see personal data section).

Section 3 – Software use

As a Group we have multiple agreements in place for the purchase of standard desktop software (for example Microsoft Office) and all software must be procured with prior written approval from your local IT Department. Users must not knowingly download software without prior approval from your local IT Department. Exceptions to this are users working in a software development capacity, who may download drivers and/or patches as part of Group related development work. Users who develop software for Vitec must refer to the recently implemented software development policy.

Software duplication or transmission

Users may not duplicate any licensed software or related documentation for use either on the Group's premises or elsewhere unless the Group has been expressly authorised in advance to do so by agreement with the licensor. A duplication of licensed software is a breach of the license agreement and will lead to financial penalties for the Group.

Users may not give software to any third party. Group users may use software on the local area network or on multiple machines only in accordance with applicable license agreements.

Transfer of software licenses

No user may sell, lend, sublicense, transmit, distribute, give or otherwise convey or make available software or interest therein to any unauthorised individual or entity without permission from your local IT Department.

Software de-compilation

No user may de-compile, reverse engineer or disassemble software unless permission has been explicitly granted in advance by the software copyright owner.

Software Installation or Removal

Only members of your local IT Department or authorised users are allowed to install or uninstall software on personal computers and servers. This includes, but is not limited to, commercial software, shareware software and freeware software.

Group developed software may be installed by individuals but only after prior (written or email) approval from your local IT Department.

Personal software may be installed with prior (written or email) approval from your local IT Department. Your local IT Department may ask for proof of ownership if software is installed on Group equipment. All software license information must be logged with your local IT Department.

Software Registration

When software is delivered, it must first be properly registered with the software publisher via procedures appropriate to that publisher. Software must be registered in the name of the company and department in which it will be used. Software must never be registered in the name of the individual user.

Software Licensing

Your local IT Department shall keep all original copies of licenses for all software used within the Group.

Software Audits

To ensure that the Group complies with all software licenses, your local IT Department will conduct periodic audits of all of computing facilities that includes but is not limited to Group supplied desktops, laptops, tablets and phones. Audits may be conducted at any time by your local IT Department, without users being given prior warning. Employees must comply with all requests for information and access during these investigations. Audits will be conducted using an auditing software product.

Software for which there is no supporting registration, license, and/or original installation media will be removed from the user's computer.

Apps

You may download apps to your work mobile phone or tablet that are either work related or assist you in performing your work. Examples of non-work-related apps which you may download may include LinkedIn, travel apps, news apps, taxi apps, etc. The cost of work-related apps can be claimed via expenses if they have been authorised by your IT Department and line manager in advance. All other apps must be paid for by the employee. You should not download apps to your work mobile phone or tablet which are unrelated to your job or which may be in violation of the Group’s Code of Conduct.

Copyrights

Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and may not copy, download, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner (see section on software use).

Section 4: electronic communication

This part of the policy outlines the Group's rules regarding the acceptable use of electronic communications.

The following rules apply to all electronic communications including but not limited to email, posts on social media sites, instant messaging and text messaging that are:

- Accessed on or from the Group's premises;
- Accessed using the Group's computer equipment, or via the Group's paid access methods;
- Used in a manner which identifies the individual within the Group.

Inappropriate content or use

The list outlined below is merely indicative and not exhaustive of conduct that may result in disciplinary proceedings. Employees should be aware that the Group may inform the appropriate authorities if, for instance, there has been a criminal offence or breach of data protection legislation or the Group believes an offence may be likely to be committed. Electronic media may not be used for knowingly transmitting or storing any communications or information that:

- Is of a discriminatory or harassing nature;
- Is derogatory to any individual or group or otherwise could bring the Group or its employees into disrepute;
- Is obscene or X-rated, or which pose a risk to the Group that they may be regarded as such and, in particular, pornographic material must not be received, stored or distributed either internally or externally;
- Is of a defamatory or threatening nature; and/or
- Is a "chain letter" or junk or spam email;

Electronic Communication and Legal Liability

Employees should be aware that the legal responsibility for employee written emails and indeed for any internet misuse by an employee rests with both the Company and the individual(s) responsible. There is a general perception that electronic communication is an informal form of communication and that it is not legally binding, however, employees should be aware that this is not always the case and in certain circumstances there might be legal liability. Electronic communication can be the equivalent to issuing a letter on the Company's letterhead and, for the avoidance of doubt, employees should be aware that this type of communication may be capable of forming or varying a contract.

Employees should, therefore, assume that electronic communications are legally binding on the Company and should take the same degree of care in relation to this type of correspondence (both external and internal) as they would in relation to formal correspondence on Company letterhead. You should not enter into any form of contract or initiate any purchase or sale electronically on behalf of the Company unless and until all normal authorisation procedures have been complied with (for example the Group's Delegated Powers and Levels of Authority).

Please be aware that when using email communication. In particular, you must use the correct email signatures that have been issued by the Group or your Division. This is a legal requirement. Please contact the Group Head Office or your Divisional Marketing Director should you need confirmation of the correct format of your email signature.

Guidelines for Electronic Communications

Good communication should involve talking to your colleagues, suppliers and customers. Often issues can be resolved much more quickly and with less chance of misinterpretation. However, where an email is a

more appropriate form of communication both internally and externally, for example when a supporting document and explanation is required, the following guidelines should be followed.

Email communications are often perceived as being closer to informal speech rather than formal writing. Messages can be sent quickly and often with little thought regarding their contents. In addition, email and instant messaging is increasingly the principal form of tangible contact between the Group and its customers and/or suppliers and, as a result, it may have a fundamental impact on their impression of the Group. In order to minimise offensive or harassing communication and to protect the Group's reputation the following guidelines must be adhered to:

- Electronic communication should be written in an appropriate tone using normal business language reflecting the standards normally adopted for letter headed paper correspondence;
- The subject field in emails should contain a meaningful description of the content of the email and emails should only be sent to persons who need to see the email;
- The inappropriate use of upper case in electronic communication is generally interpreted as SHOUTING and should be avoided;
- Employees must not abuse others even in response to abuse directed at them;
- If a user receives an email or electronic communication in error, they must inform the sender immediately and delete the message from their mailbox or conversation history;
- Emails must include the appropriate legal information such as Company name and registration number. Templates have been issued by the Group and must be used.

Electronic Communication Monitoring

There is a general expectation that all correspondence via email is secure and private. However, the Group, for legitimate business purposes, may monitor electronic information created, stored and/or communicated by an employee, though the Group will respect the individual's privacy within the terms of this policy. The following should be noted:

- The Group routinely monitors usage patterns for both voice and data communications (for example the number called, or website accessed, call lengths, frequency of calls etc.). This type of monitoring allows the Group to perform accurate cost analysis, better financial allocations and to actively manage the systems required to provide the various technology services.
- The Group reserves the right, in its discretion, to review any employee's electronic files and messages (email/instant messaging history) and usage to the extent necessary to ensure that the Group provided services are being used in compliance with the law, to protect the Group's reputation and to protect the stability of the Group's computing environment.

Employees should, therefore, not assume electronic communications are totally private and confidential. Personal use is at the discretion of the Group and employees found to be abusing these facilities may have their rights removed.

Employees on holiday or who have left the Company may have their email mailboxes or instant messaging conversation history files opened and searched for business related communications. With regards to personal privacy as listed within the Human Rights Act (1988), communications which are clearly of a personal nature will not be accessed or disclosed by the Group.

Email and Instant Messaging Housekeeping

Employees are encouraged to practice good housekeeping with regard to email and/or instant messaging services, especially given that individual storage space restrictions are in place. It is the employee's responsibility to store only items that may be required for retrospective access. It is recommended that frequent archiving of emails is carried out, and that data that is business sensitive or critical should be

categorised and saved in a suitable location for the employee or employees to access. Users who require guidance in performing housekeeping duties should contact your local IT Helpdesk to arrange for training.

Social Media communication

The use of Social media websites and applications has expanded dramatically over the last few years. This form of electronic communication can be a concern for employers and employees in that it:

- Has the potential of being instantly and universally publicised, or disseminated;
- Has the potential to be communicated to a much wider audience than originally intended;
- Has the potential to be irrevocable.

While the Group does not, in any way, seek to impose its view of the "proper" use of these forms of communication on any of our employees, the fact is that where we, as employees, are either speaking of matters involving our work or are identified as representing the Group, it is easy for a reader of a Facebook page, a Twitter tweet, your LinkedIn profile or an email to identify what is being said as being a position of the Group for whom you work. Therefore, we believe it responsible and appropriate that employees adhere to the following:

- It is each employee's responsibility to know and adhere to The Vitec Group Code of Conduct.
- Each employee must understand that you are each personally responsible for what you publish online – whether that be Twitter, Facebook, LinkedIn or any other forum.
- What you put on to the web will be public for a long time – you should protect your privacy and the privacy and interests of the Group and your fellow employees.
- You must identify yourself (your name and if appropriate your role within the Group) when you discuss Group related matters. Write in the first person. ("I" not "We") and you must make it clear that you are speaking for yourself and not on behalf of the Group. It must be made clear at all times that you are expressing your personal opinion.
- If you put any content on to any website external to the Group and that content has something to do with the work you do or any subjects associated with the Group, you are required to use a disclaimer such as this:
  "The postings on this site are my own and do not necessarily represent the positions, strategies or opinions of The Vitec Group plc or any of its subsidiary companies."
- Copyright, trademark, fair use and financial disclosure laws apply to you as much as they apply to the Group.
- Do not provide anyone's confidential or other proprietary information on any submission. You are required to request and receive specific prior written permission to publish or report on matters that are private or internal to the Group.
- Do not cite or reference our clients, partners or suppliers without their specific prior written approval. When you do make a reference, where possible link back to the source.
- Be aware of your association with the Group in all online social networks. If you have identified yourself as a Group employee, ensure your profile and related content is consistent with how you wish to present yourself to colleagues and clients. Again, keep in mind that you are always required to conduct yourself with the published Code of Conduct and in all situations where that conduct could conceivably reflect upon the Group.

When posting, tweeting or commenting on any work-related activity, the following rules apply:

- Factual statements about Group Products are acceptable. Example: Our new battery is half the weight of our prior battery.
- Factual statements about the use of Group products are acceptable. Example: Camera Corps used the Qx Com Cam kit to cover the 2019 Rugby World Cup in Japan.
- Opinion statements about our products that are clearly denoted as the authors are acceptable. Example: I (the author) believe that our light provides the most colour accurate artificial lighting available.

- Opinion statements reflecting on any other competitor product or competitor are not acceptable.
- Statements that state, imply or infer endorsement are not acceptable. Example: NBC loves the Vision blue3 with its perfect balance and infinite drag control. Unless specifically (and in writing) agreed to by the entity providing the testimonial.
- Statements as to other products – of any nature – are not acceptable.
- A statement comparing operational capabilities of a Group product verses a competing product is not acceptable.
- Statements quoting anyone (even in paraphrase) (without a specific written agreement from them verifying the quote and its publication) are not acceptable.
- Statements denigrating any other products, people or company are not acceptable.
- Statements that are immoral, lewd, profane, or otherwise objectionable are not acceptable.
- Statements that mention any sensitive Group information are not acceptable.
- Without specific written approval from the Group Company Secretary, no statements whatsoever may be made regarding, but not limited to: acquisitions, disposals, contract “wins”, contract “losses”, negotiations with any prospective customer, products in development, employees, internal policies, movements, plans or designs.
- Employees are not permitted to post any statements about the Group’s current or future performance, financial information or share price performance.

Section 5: Personal Data

Managing personal data

Personal data applies to data in any format that may directly or indirectly identify a natural person. This data takes many forms, including, but not at all limited to: a name, a postal address, a birthdate, email address or even an IP address. Any personal data which you are handling needs to be treated with great care. Most importantly it must have been obtained for a legally valid purpose and with the person's consent. It needs to be kept safe and secure – this includes hard/soft copy files and documents.

When communicating personal data ensure that you restrict data to only what is necessary. In addition, any personal data sent should be encrypted by any practical means, such as a password on the file.

When there is no longer a legitimate reason for keeping personal data, it should be deleted. This includes any emails containing personal data. You may at any point be required to clearly identify any personal data which you hold, where this is held, and the rationale for maintaining such information.

Dealing with breaches

If you become aware of a personal data breach, the standard breach reporting procedures must be adhered to, as outlined in section 2. You must immediately notify your IT Department, nominated Data Protection Lead and the Group's Company Secretary. They will assess and initiate the next steps.

Under GDPR, there may be a requirement to notify the relevant data protection authority within 72 hours of the personal data breach being discovered, therefore immediate escalation is required for Group to make an assessment of any personal data lost.

"Subject Access" Requests

Any individual (Data Subject) has a legal right under European data protection law to be informed whether personal data is processed (which includes being held or stored); a description of the data held; the purposes for which it is processed and to whom the data may be disclosed; a copy of the information constituting the data; and information as to the source of the data. This must be provided by the Group within 30 days of the request date.

If you receive a Data Subject access request, you must immediately pass this on to your responsible Data Protection Lead who will coordinate the response, confirm the identity of the Data Subject and start a log/tracking sheet detailing the date the request was received and when each stage of the request was completed.

The Data Protection Lead will contact all holders of data (i.e. the relevant Departmental or functional lead) to search for both manual and electronic information. The registered holder will be responsible for checking systems (including computer held records), emails and files for any reference, directly or indirectly, relating to the Data Subject.

Third parties (data processors)

In many cases we transfer personal data to a third party which we then refer to as a "Data Processor". This includes our outsourced payroll providers, pensions and share incentives providers, digital marketing providers and any other company which is entrusted with personal data.

If you are responsible for a contractual relationship with a Data Processor, you must ensure that adequate safeguards are in place to ensure that the data is safely looked after. Your Data Protection Lead will be able to advise on the arrangements including contract terms to put in place.