LIBERTY INDUSTRIES GROUP
POLICIES & PROCEDURES

Policy Title	A10. Electronic Communications
Employer/Company ("Business Unit")	LIBERTY INDUSTRIES GROUP HEAD OFFICE - OLDBURY
Business Unit Compliance Officer ("BUCO") if applicable	

Issue Record

Issue No.	Effective Date	Authorisation	
		Name	Position
1	February 2016	Head Office	
2	May 2017	Head Office	

Electronic Communications Policy

Introduction	This policy sets out rules relating to the use of the Company's computer, telephone and facsimile facilities, including Company laptops and mobile telephones. It applies to all users of the Company's telecommunications systems and should be read in conjunction with the Company's Disciplinary Policy, Mobile Phone and Data Protection Policy. Any breach of this policy will be taken seriously and may lead to disciplinary action, which could include summary dismissal, under the Company's Disciplinary Procedure. If you are unclear about the effect or meaning of any part of this policy, you should seek clarification from an administrator before you use the Company's electronic communications systems. This policy may be changed from time to time.
Purpose	The purposes of this policy are: to ensure that computer and telephone resources are used properly; to set out rules on the personal use of computer and telephone resources; and to inform employees of the way in which communications may be monitored.
Scope	The Company's policy applies to all its employees and to everyone working at its premises, including any contractors. Managers are responsible for ensuring that those reporting to them have read and understand this Procedure before access to IT Resources is provided. Managers are also responsible for working with their HR representative to initiate appropriate disciplinary action in the event of non-compliance.
Computer Use	
Introduction	The use of the Internet, e-mail (both internal and external) and the computer system carry serious risks for the Company. E-mail, although often seen as an informal method of communication, should be seen as equivalent to writing a letter on Company paper. Careless use of the Company's e-mail and Internet system can have serious consequences. For example, it

	is possible to create a legally binding contract by exchange of e-mail and confidential information may be deliberately or accidentally sent to the wrong people. In addition, misuse of the Internet and e-mails can introduce viruses into the network, infringe copyright laws and result in the harassment or defamation of others. For these reasons, the Company imposes strict limits on Internet and e-mail use in relation to both business and personal use.
Viruses	The introduction of viruses into the Company's computer system is potentially devastating. Although the Company has installed anti-virus software, this does not guard against all viruses. Users should be aware that viruses could be introduced via e-mail attachments, CD-ROMs, mobile phones, floppy disks, memory sticks, DVD'S, their storage media and the Internet. It is the user's responsibility to take care when opening e-mail attachments especially when they are not expected or from unknown sources. If in any doubt, please contact an administrator who will check whether it is safe to open the attachment. You should never open attachments ending with '.exe, .vbs, or any types of executable or compressed file without obtaining clearance from an administrator. You must not install any software that has not been purchased by the Company and approved by the IT department. Only storage media, such as DVD's, memory sticks etc., supplied and approved can be used on the IT Network
Security	You should not download any material, including, but not exclusive to, games, screen savers, files and mp3's from the internet, CD-ROMs, memory sticks, mobile phones, DVD's, floppy disks or other storage media without the approval of an administrator.
Wireless technology	Everyone who has a Company laptop will be advised by their IT representative whether it can be used via wireless technology. This is only allowed if the appropriate security software and encryption are in place.
Travelling	Given the amount of confidential information which is accessible on our equipment, you must take sensible precautions when

	you take laptops, smart-phones and PDAs out of the office. In particular, you must never leave one of our laptops, smart-phones or PDAs on view inside a vehicle. If you have to leave such an item unattended in a vehicle, it must be locked away in the boot or glove compartment. If you are traveling on public transport or are in a public place, keep your laptop, smart-phone or PDA with you at all times or, if this is not possible, in sight. Remember that thieves specifically target laptop-carrying cases. If you are working in a public place, be aware that other people may be able to read documents that you are working on.
Passwords	The system requires users to change their password regularly. Do not divulge your password to others. You should not use a workstation without authorisation or use another person's password. You must log out of or lock your terminal when it is not in use or you are away from the desk. If service or support is required, passwords may be shared when you are certain that the person is a member of your IT Department, but must be changed immediately afterwards. Your PC/Laptop should be manually locked when your system is unattended
E-mail Content	It is very easy to send an email to the wrong person. You should be very careful to ensure that the emails you send are correctly addressed particularly when they contain information that you would not want others to see. Remember that email is not a secure way of sending information. Emails can be intercepted by third parties and intended recipients can alter and/or forward emails without your knowledge. You should therefore avoid sending by email personal information about individuals or commercially sensitive information. If you have no choice and you have relevant approval, you must use the privacy setting. Contact an Administrator for assistance if required. • Remember that deletion from your inbox or archives does not mean that emails are destroyed, and at times we may need to retrieve them. Email messages may be disclosed in legal proceedings in the same way as paper documents. • When sending e-mails, internally or externally, you should exercise the same care as if you were sending a

	letter on Company headed paper. • You must not send, forward, distribute or retain e-mail messages that contain language that is abusive, aggressive or offensive. You must not make any improper discriminatory reference to a person's race, colour, religion, sex, age, national origin, disabilities or physique, when writing e-mails and must not forward or distribute any material that does so. If you receive any messages you are unsure about, you should contact an administrator who will tell you what you should do. • The effective operation of the network can be hindered when large attachments, such as video clips or pictures, junk mail, hoax virus warnings and e-chain letters are sent and received. You must not send and should not ask others to send such information to you for non-business purposes. • It is possible to create legally binding contracts without intending to via e-mail correspondence. E-mail must not be used for communications that could lead binding contract being formed or which would have the effect of obligating the Company in any way without prior authorization/approval being given from the relevant manager. The following standard email signature will be used using Font Calibri**:** Name Title Business name DD: +44 (0) …… Tel: +44 (0) …… Fax: +44 (0) …… Email: …… Website: www..com Correspondence Address: …… ……

	A trading division of ……. Ltd. Registered Office: Registered in England No …….. This email and any attachments are confidential. If you are not the intended recipient, please notify the sender by reply email and then delete it from your system immediately. Any disclosure, copying or distribution of the message or any action taken or omitted to be taken in reliance upon it is prohibited and may be unlawful.
Copyright	Most information and software that is accessible on the internet is subject to copyright or other intellectual property protection. Nothing should be copied or downloaded from the internet for use within the Company unless the material owner has given express permission.
Hardware/Software	Only authorised and properly licensed hardware and software can be used. A system administrator should be contacted to install any necessary software. Under no circumstances should unauthorised hardware be introduced onto the local network. This includes, but is not exclusive to, laptops, mobile phones, PDA's, network devices, external drives, wireless devices, USB memory sticks etc.
Personal Use of Company Computers	The Company's computers, including laptops, are to be used solely for business purposes, subject to the following exceptions; • You may make reasonable use of the Company's computer system for sending personal e-mails outside of your normal working hours or during your lunch break in accordance with the terms of this policy; • You may use the internet for reasonable personal use (except for accessing social media websites) outside of you normal working hours or during your lunch break in accordance with the terms of this policy; The Company reserves the right to withdraw permission for personal use in individual cases without giving reasons.

Mobile Devices	Mobile Devices have arisen as powerful computing devices with access to important company and personal information. For any personal mobile device accessing Liberty email or data follow these rules to keep our Company and your personal information safe: Implement safeguards to protect your personal mobile device (e.g., passcodes, encryption, lockout after failed login attempts and inactivity timeout). Contact your IT Department if you need help with these safeguards. Do not circumvent mobile device security controls (e.g., passcodes, encryption, lockout after failed login attempts and inactivity timeout). Protect the physical device by keeping it in a safe location, and avoid leaving the device unattended in a motor vehicle or in a public area. Observe all applicable laws, including all such laws restricting the use of mobile devices while driving. Only install personal applications with a good reputation from a reputable source. Consult IT before installing applications if there is any uncertainty. Immediately report loss or theft of the personal device to your IT Department. Regularly backup the information and the applications on the device.
Inappropriate Websites	You must not under any circumstances access inappropriate or offensive websites or distribute or obtain similar material through the Internet or e-mail when using Company equipment, even if you are doing so in your own time. Examples of inappropriate or offensive material include racist material, pornography, sexually explicit images, text and related material, the promotion of illegal activity or intolerance of others, gambling sites and chat rooms. You should remember that although one person does not find certain material offensive, another might. The Company has the final decision as to whether it considers particular material to be inappropriate under this policy. Any user who is unsure whether particular material would be considered appropriate by the Company should seek clarification from a manager or administrator before accessing or distributing such material. If in any doubt as to whether the Company would consider certain material inappropriate, do not

	access or distribute it. If you receive material that contains or you suspect contains inappropriate material or you access such material on the Internet inadvertently, you must immediately report this to your manager or an administrator who will tell you what to do. You must not under any circumstances forward, show to anyone else or otherwise distribute the material. Software on the network servers will limit access to various blocked websites and this "block list" will be regularly updated. If you require access to blocked websites contact an Administrator.
Third Party Services (including "Cloud" providers)	Anytime a third party IT service or cloud storage provider collects, store, process, transmit or access Liberty's information, a contract must be entered into and an information security review must be performed prior to entering into a contract. Examples of third party services include, but are not limited to: support for marketing campaigns, payroll processing, talent management, website hosting, data center facilities and remote support for Company IT resources. The review will ensure that we will have acceptable levels of risk to the confidentiality, availability and integrity of Company information. Liberty is ultimately responsible for the information's security while it is in the care of a third party.
Social Media	In relation to this policy, all forms of social media, such as Facebook, Twitter and other social networking sites and blogs, will be subject to the following. Personal use of social media at work is not permitted. Inappropriate use of social media which has an adverse impact on the company, its employees, customers or suppliers is also prohibited even if carried out in an employee's own time. Social media must not be used in a way that breaches our policies or breaches any other laws or ethical standards. Employees who access social media sites using our IT systems should note that these are our property and that social media posts may be monitored.

	Employees must not make posts on social media websites that: • Are disparaging or defamatory towards the company, employees, clients and suppliers • Are damaging to our business reputation • Are personal views which appear to be the views of the company • Disclose confidential information • Use our logos, brand names or other company trademarks • Contain any remarks that may be construed as offensive, discriminatory or obscene towards any employees or workplace contacts Employees who breach these rules will be subject to disciplinary action up to and including summary dismissal.
Public File Transfer	Public File Transfer services, such as DropBox, WeTransfer and YouSendIt or even FTP service, are only to be used when sending large file attachments that exceeds the limitation of our email system. Usage of this type of tool must be coordinated with the IT department and should only be used as a sharing resource. Users should immediately delete the data once successful transmission has occurred. Storage of company related data online while using these tools is strictly prohibited.
Personal Use of the Telephone	This policy applies to land lines and to Company mobile telephones. You are permitted to make reasonable private telephone calls during your lunch hour or outside of working hours. The following types of personal calls are never permitted: calls to premium lines, calls to chat lines and unauthorised overseas calls.
Auditing and monitoring	To ensure compliance with Company policies and meet legal obligations, Liberty reserves the right, within the boundaries of applicable law and in a manner consistent with our established employee and Safe Harbor privacy policies, to: Inspect and possibly disclose information processed on Company IT resources. Inspect information stored on employee-owned mobile

	devices that connect to Company. Remote wiping of mobile devices when instructed by HR and or Senior Management. Inspect computing devices for security vulnerabilities. Monitor network communications. Monitor file transfers. Monitor Internet Browsing
Recordings	You are not permitted to record, by means on any device, any meeting or telephone call between yourself and any other Liberty Commodities employee or group of employees, or any customer or supplier, without the express written consent of a manager. If it is found that you have created a recording which has not been authorized you will be liable to disciplinary action, the outcome of which is likely to be the termination of your employment. In addition, in those circumstances the Company may require you to destroy the recording in question, and to evidence to its satisfaction that you have done so. You may be asked to surrender any device that the Company reasonably believes is capable of creating a recording for the duration of any meeting if the Company reasonably believes you intend to record it without authority. This rule does not act so as to prevent you reporting matters of public concern; however, before taking any action you should refer to our "Public Interest Disclosure" Policy.
Photography	You are prohibited from making any photographic record, whether still or moving, of any Liberty House Groups premises, processes, or employees unless you have express written consent from a manager to do so. If you create a still or moving image in breach of this rule you will be subject to formal disciplinary action, the outcome of which is likely to be the termination of your employment. In addition, in those circumstances the Company may require you to destroy the image or images in question, and to evidence

	to its satisfaction that you have done so. This rule does not act so as to prevent you reporting matters of public concern; however before taking any action you should refer to our "Public Interest Disclosure" Policy

Your right to access	We may disable your access to any telecommunication system, including email, at any time. We will only do so with good reason, for example if you give or have been given notice of the termination of your contract.
Data Protection	Electronic data is stored in accordance with the Data Protection Act as detailed in the Data Protection Policy.
Status of this policy and new instructions	This policy does not give contractual rights to individual employees. The Company reserves the right to alter any of its terms at any time although we will notify you in writing of any changes. This policy may be supplemented by additional instructions from the IT department about how you use our telecommunication systems. It is very important that you comply with any such instructions.