

PECCU

Policy on Electronic Communications & Computer Use (PECCU)

Rule: PECCU (Policy on Electronic Communications and Computer Use)

Issue Date: 25th February 2019

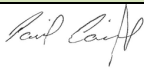
Purpose: This document defines the acceptable use controls that are to be applied when using or accessing ScottishPower Cyber-Infrastructure (see Definitions in this document) electronic devices, network resources, and information assets.

Owner: Human Resources

Custodian: Cyber Security UK

Updating the Rule: Annually, the Owner(s) shall review and update the Rule and associated attachments, as necessary. Substantive changes in the Rule shall be reviewed and validated by the owner and re-approved.

Approvals:

Status	Date	Name	Title	Signature
Approved	10 th December 2018	Paul Cairns	Head of Cyber Security	
Approved	10 th December 2018	Sarah McNulty	Director. HR Operations	Email

Version History:

Version	Status	Author	Reason for Issue /Change	Date
1.0.0	Final	L Cuthbertson	Initial Document	01 Aug 2012
1.4.0	Interim	E Eren	P Cairns Review	12 Oct 2017
1.4.4	Interim	E Eren	HR Copy for Review	19 Oct 2017
1.5.0	Review	R Berends	HR Review	17 Nov 2017
1.5.3	Draft	R Berends	HR & UK IT Security Updates	25 Jan 2018
1.5.5	Draft	R Berends	Definition Updates, Collaboration Section	14 Mar 2018
1.5.6	Draft	R Berends	Alignment with Information Management Rule / GDPR	09 Apr 2018
1.5.7	Review	R Berends	Review Copy for HR	13 Apr 2018
1.5.8	Review	R Berends	Review HR Updates for Cyber	30 Apr 2018
1.5.9	Final	R Berends	Final Review for HR & Cyber	15 May 2018
1.5.10	Review	Pau Cairns	Updated following HR review	18 May 2018
1.5.11	Review	R Berends / Paul Cairns	Updated	06 July 2018
1.5.12	Review	Paul Cairns	Updated to include Binding Corporate Rules	09 August 2018
1.5.13	Review	Paul Cairns	Updated following review	27 September 2018



2.0	Approved	Paul Cairns	Approved	10 th December 2018
2.01	Draft	Scott McGowan	Minor update; correct grammar, update references to 1HR to 1HR Direct, remove references to IEC and the Regulation of Investigatory Powers Act.	15 th January 2019
2.02	Draft	Erdem Eren	Minor update; remove references to relating rules throughout the PECCU, additional suite of related rules in compliance section.	05 th February 2019
2.03	Draft	Sarah Young	Minor update; minor grammar and spelling corrections.	12 th February 2019
2.04	Final	Paul Cairns	Minor updates, finalised Live version	25 th February 2019



Contents

1.	Purpose and Aims	6
2.	Scope.....	6
3.	Rule Principles and/or Requirements.....	6
3.1.	Definitions	7
3.2.	Electronic Communications and Equipment.....	8
3.2.1.	Electronic Communications Standards.....	8
3.2.2.	Equipment Rules and Requirements.....	8
3.2.3.	Use of Equipment not Owned by ScottishPower.....	10
3.2.4.	Misuse of Electronic Communications and Equipment.....	10
3.2.5.	Storage Media.....	11
3.2.6.	Use of Equipment/Data Offsite.....	11
3.2.7.	Data Protection	12
3.2.8.	Data Classification, Handling and Transfer; Rules and Requirements.....	13
3.2.9.	Disposal of Digital Records.....	14
3.2.10.	Clear Desk and Device Screen.....	14
3.2.11.	Limited and Reasonable Personal Use.....	14
3.2.12.	Offensive or Defamatory Material.....	15
3.3.	Access Control	16
3.3.1.	Access Management Requirements.....	16
3.3.2.	Users Changing Role or Leaving.....	17
3.3.3.	Logins and Passwords/Passphrases.....	18
3.3.4.	Choosing a Password.....	18
3.3.5.	Password Policy.....	19
3.3.6.	New IT Systems.....	19
3.4.	Electronic Communication Tools	20
3.4.1.	Instant Messaging Rules and Best Practice.....	20
3.4.2.	Collaboration Network Rules and Best Practice.....	21
3.4.3.	Email Usage Rules and Requirements.....	21
3.4.4.	Prohibited Use of Email	22
3.4.5.	Effective Use of Email	23
3.4.6.	Email Disclaimer	23
3.5.	Use of Company Internet and Intranet	23
3.5.1.	Effective Use of Company Intranet & Internet	23
3.5.2.	Prohibited Use of Company Internet.....	24
3.5.3.	Social Engineering	25
3.5.4.	Social Networking.....	25
3.5.5.	Private Use of Social Networking	26
3.6.	Virus, Encryption and Malicious Communications	26
3.6.1.	Computer Virus	26
3.6.2.	Encryption.....	27
3.6.3.	SPAM and Phishing.....	27

3.7. Monitoring	28
3.7.1. Privacy of Electronic Communication and Physical Storage	28
3.7.2. Monitoring Methods	28
3.7.3. Investigations	29
4. Roles & Responsibilities	29
4.1. All Users	29
4.2. Managers	29
4.3. Human Resources	30
4.4. Cyber Security	30
4.5. Corporate Functions and Business Areas	30
4.6. Reporting	30
5. Compliance	30
5.1. Compliance Measurements	30
5.2. Compliance Mapping	31
5.3. Related Company Rules and Policies	31
5.4. Non-Compliance	31
5.5. Guidance and Useful Contacts	32



1. Purpose and Aims

The Company's (defined in "Definitions" below) electronic communications and computer resources are valuable Cyber Assets (defined in "Definitions" below) and critically important operational tools. To ensure the efficient, legal and professional use of these resources, the Company has developed the Policy on Electronic Communications and Computer Use (PECCU).

The PECCU is a key employment policy which you are required to read in order to understand what you may and may not do in relation to use of the Company's Cyber-Infrastructure (defined in "Definitions" below). You must comply with all aspects of this policy and the related Rules and you should discuss any queries about it with your line manager in the first instance.

The Policy:

- Protects the Company and individuals against data loss
- Protects Users (defined in "Scope" below) from the risks associated with using electronic communications and computer resources
- Requires responsible and efficient use of the Company's electronic communications and computer resources
- Maintains the confidentiality, integrity and availability of the Company's Cyber-Infrastructure
- Safeguards against damage to the ScottishPower brand and reputation
- Promotes compliance with all applicable laws and regulations, including General Data Protection Regulations (GDPR), Copyright and Licensing Laws.

You should be aware that it is the Company that considers if there has been a breach of the Policy and you may be subject to action under the Company's Disciplinary procedure, which could result in termination of your employment.

For the avoidance of any doubt, the Company shall be the sole determiner of what constitutes a breach.

2. Scope

This Policy applies to all:

- ScottishPower employees (permanent and fixed term contract)
- Temporary staff on work experience/student placements
- Agency staff
- Suppliers (including independent Contractors and Subcontractors) where their activities require them to work on ScottishPower premises or otherwise access ScottishPower systems and information.

Throughout the PECCU, all of the above personnel types are referred to as "Users". All Users shall be required to read and acknowledge their understanding of the PECCU.

The PECCU and subsequent process applies to the Company and future subsidiaries, affiliates and holding companies. Where applicable, the PECCU should be used in conjunction with the corresponding Rules.

Occasionally users and/or the organisations may request exceptions to these policies, rules or standards, where the risk (in terms of cost, time, operations, technology) to be compliant with, significantly exceeds the risks of non-compliance. Exception requests made in accordance with the ScottishPower Exception Management Rule shall be considered, provided that the alternative presents a reasonable and justifiable business case for the exception, including the use of compensating controls and the existence of appropriate resources to properly implement and maintain alternative technologies and processes.

3. Rule Principles and/or Requirements

This policy is primarily to ensure the efficient, legal and professional use of the ScottishPower information and technology systems. It is based on a number of Rules which contain the full detail of specific topics as referred to in this document. Within each section, this document highlights the most pertinent points from the Rule/s, as well as guidance on best practices and usage tips. The relevant rules are listed at the end of this document.



3.1. Definitions

Throughout this document, a number of specific terms are used which are defined as follows:

“Iberdrola”, “ScottishPower”, “Company” and “Group” are all terms meaning any of ScottishPower and/or Iberdrola’s businesses and all companies within the ScottishPower group.

“Policy” shall mean this document and all related Company Rules referenced herein.

“Act” is the Data Protection Act of 2018

“GDPR” is the General Data Protection Regulation of 2018.

“Equipment” includes, but is not limited to; Personal Computers (PCs), workstations, laptops, networks, fixed/mobile telephony equipment, electronic tablets, Smart phones, Smart watches, hand-held wireless devices, printers/copiers, scanners/faxes, Storage Media (as defined below), Data Capture Devices, remote access key fobs and CCTV.

“Portable Devices” includes, but is not limited to; Laptops, mobile telephony equipment, electronic tablets, Smart phones, Smart watches, hand-held wireless devices and Data Capture Devices.

“Storage Media” shall mean all media including, but not limited to; hard disk drives, floppy diskettes, optical discs (including CD, DVD, Blu-Ray and all other types of laser read and/or write discs), USB flash drives, SD, MicroSD and all types of flash memory cards.

“Cyber Assets” includes, but is not limited to, all electronic information and communications systems, physical security systems and the information contained in these systems.

“Cyber-Infrastructure” means all Cyber Assets, Storage Media and Equipment, as well as the related services, security systems and software that process (create, access, modify and destroy), store (paper, magnetic, electronic, and all other media types), and communicate (sharing and distribution) information, or any combination of these elements.

“Social Networking” shall mean distributing information, comments and messages via Internet or Intranet systems. Examples include participating on social network sites, using network collaboration tools, posting in forums, posting on message boards and tweeting, all of which are on-line systems where users may create posts, participate in discussions or post other content.

“Electronic Messaging” includes, but is not limited to; Social Networking, sending email, using webmail (web-based email), sending SMS texts, picture messages, instant messaging, chat rooms, blogging and video logging (vlogging).

“Electronic Communications” includes, but is not limited to; Electronic Messaging, Social Networking, scanned documents, telephone calls, faxes, voicemail messages, data network, intranet and Internet access/use.

“Personal Data” is defined in the Act and GDPR as “data which relate to a living individual who can be identified from that data alone or from that data and other information which is in the possession of, or is likely to come in possession of, the data controller”.

Personal Data includes employee as well as customer data and can be factual (such as a name, address, date of birth, telephone numbers, job title, account number, National Insurance number, health information, financial data and/or bank details or email address), or it can be an opinion or a statement of intention. Even if an individual’s name is not given, information can still be Personal Data if there is enough information to identify the individual.

Personal data can be stored on paper or Storage Media and is subject to certain legal safeguards specified in the Act and the GDPR.

“Protected Information/ Data” is information/ data created, received, transmitted or stored, that due to its nature or value to the company is subject to enforced protection measures, including but not limited to Personal Data, commercially sensitive information, critical infrastructures information, strategic business information, credential data, encryption keys to systems and applications, or any information that could be subject to special protection under any external regulation.

“Staff” includes all ScottishPower employees, (permanent or fixed term), temporary staff on work experience, student placements and agency staff.



3.2. Electronic Communications and Equipment

The ScottishPower Cyber-Infrastructure has been built to support the Company's business and this policy has been written to ensure the efficient, legal and professional use of the facility.

3.2.1. Electronic Communications Standards

Legal Standards

From a legal standpoint, all Electronic Communications, issued using Company Equipment, have the same permanence and authority as written communications. Therefore, all communications issued must be treated as if they were issued on Company headed notepaper and must meet the standards expected of written communications.

Accuracy of Electronic Communications is especially important when dealing with external organisations. You should remember that when you send any communication through the Company's Equipment, you are representing the Company. It is possible to make a legally binding contract or give rise to expectations via email and other Electronic Communications. When communicating with other organisations, you must be aware of the danger of inadvertently changing the terms of existing contracts or even creating new contracts on behalf of ScottishPower and should only send Electronic Communications for which you are properly authorised.

You should also be aware that any advice given to customers or other third parties via all forms of Electronic Communications is subject to the same risk of claims for negligence as any other means of communication and care should therefore always be taken.

You should also remember that Electronic Communications, in particular emails, no matter how confidential or damaging, may be disclosed in any legal proceedings or regulatory investigations involving the Company.

Information received by Electronic Communications should be treated in the same way as all other written correspondence and should only be forwarded or further disseminated for defined, specific business purposes.

Other Legal Considerations

Prior to sending Electronic Communications or accessing, receiving, transmitting or downloading material, you must use reasonable measures to ensure that you will not be in breach of Copyright, General Data Protection Regulations (GDPR) or Licensing Laws/Regulations.

If you are unclear about your legal obligations, you should discuss this with your line manager. If further guidance and clarification is required, you can refer queries to your business Data Protection Manager, the Business Systems Team or the Legal Department.

3.2.2. Equipment Rules and Requirements

It is important to ensure that Equipment is used according to its intended use. ScottishPower has a number of Rules that relate to your use of Company Equipment, these are listed at the end of this document, however the pertinent points are summarised below:

- a. ScottishPower Equipment is the property of ScottishPower and is only provided to Users for the pursuit of their professional activity, to be used in accordance with duties and responsibilities. When it is determined that the use of the Equipment is no longer necessary, it must be returned to ScottishPower
- b. The only Equipment that may be attached (on site or remotely) to the ScottishPower Cyber-Infrastructure is that which has been authorised by ScottishPower. This means that you may not attach any other Equipment (mobile phone, USB devices, camera flash memory cards etc.) to the ScottishPower Cyber-Infrastructure without prior written authorisation from Cyber Security UK
- c. To ensure adequate control and management of Company equipment, users must only procure items via Company procedures. Ad-hoc purchases of electronic communication equipment through the claiming of expenses or use of company credit cards is prohibited
- d. The company procedure for ensuring appropriate local authorisation and execution of all IT changes including access rights and equipment provisioning is the Service Request process, found under "IT Requests and Incidents" in "My Corporate Applications"
- e. You are responsible for the appropriate use and security of ScottishPower Equipment, which includes keeping passwords and other access control details secret. Please refer to the Access Control section of this document for more information. Being in breach of this Policy, or any negligent or unlawful activity shall be considered inappropriate use
- f. ScottishPower Equipment is provided with the required security configuration. You may not compromise, tamper with or attempt to circumvent this (e.g. by hacking BIOS passwords, jail-breaking Apple iOS devices or rooting Android devices)



- g. Only Company owned and procured software shall be installed on Company equipment
- h. Downloading free software or shareware by Users is not permitted. If such software is required for business purposes, it must be requested using a Service Request with License fees paid and the software will be tested prior to use. Unsupported software (often classified as “freeware” or “shareware”) may not be used
- i. You must ensure that you adhere to backup and software updating processes as well as password management requirements in accordance with Company guidelines
- j. Unless specifically authorised by exception process or by Cyber Security UK in writing, you may not store any ScottishPower owned Protected Information/ Data or Customer Sensitive Information on any Equipment not owned by ScottishPower. This extends to and includes the forwarding of emails or information to personal devices or Equipment
- k. No ScottishPower Protected Information/ Data may be removed from the Cyber-Infrastructure for any reason without prior written authorisation from Cyber Security UK
- l. Personal Data (including, but not limited to employee and customer data) must not be copied to Storage Media without prior written authorisation from Cyber Security UK **and** either the Data Protection Manager from your business, or the Data Protection Officer.
- m. When handling, processing or transferring Personal Data internationally or to other parts of the Company located outside of the UK, you must confirm with your Data Protection Manager or the ScottishPower Data Protection Officer that the appropriate legal basis and measures are in place.
- n. Users must immediately report lost, compromised, or stolen ScottishPower owned Equipment (including mobile, tablet and wearable devices) to their manager and the Service Desk in line with the “Equipment Loss / Theft Process” which can be found on the Intranet Portal under Corporate Security → Policies
- o. You must immediately notify your line manager and IT Service Desk if you become aware of any unauthorised disclosure or loss of any ScottishPower Protected Information/ Data
- p. At all times, you must protect ScottishPower Cyber Assets from unauthorised access and use by others, including family members, friends and others. Log out of (or screen lock) your device before you leave it and always ensure that Equipment is securely locked by a Kensington lock (or other anti-theft control)
- q. You are responsible for protecting ScottishPower Protected Information/ Data that you have access to, no matter how or where it is stored; electronically, reproduction image, paper or Storage Media
- r. You may not use any ScottishPower Cyber-Assets for personal use, unless specifically authorised to do so or when used in accordance with the appropriate Rule/s
- s. In accordance with the Mobile Phone Policy, personal calls or calls to premium rate numbers should not be made from Company mobile telephones or landlines
- t. All equipment provided by ScottishPower remains the property of the Company. Unauthorised use or unauthorised “borrowing” of this equipment is strictly prohibited.

Failure to comply with the rules and requirements above and those highlighted in section 5.3 may result in action under the Company’s Disciplinary procedure.

The following are recommendations and best practices that will help to ensure that you are compliant with the relevant Rules in an effective manner:

- a. The Rules are clear that only Company issued USB devices may be connected to Company Equipment, if you need to connect a non-Company issued device, please contact Cyber Security UK for authorisation
- b. Lock away Equipment in a secure place (lockers or drawers) when it isn’t in use. Never leave Equipment unattended in vehicles or other locations. If you have to leave it in a vehicle, make sure it is not in plain sight, use the boot if possible, but take steps to avoid observation
- c. Be aware that laptops and other mobile devices are fragile and susceptible to damage by rough handling, theft or extreme temperatures. Users are responsible for their Company portable devices; these can easily be stolen or lost, so should be kept with you at all times. When travelling, you must always carry your laptop as hand luggage and never check it in as hold baggage
- d. If you need to charge your mobile electronic devices, avoid using public charging stations, as these have been known to host cyber hacking tools
- e. Equipment should be switched off on completion of the working day, unless it is needed after hours.
- f. If a piece of Equipment is no longer required (i.e. when a user leaves the Company), it must be returned to IT UK, via a Service Request for “030 - Equipment & Accessories” then “010 – Remove PC” for



computing equipment or disposed of appropriately in accordance with the “Disposal of Digital Records” clause in this document

- g. Users must ensure that their laptop is securely locked by a Kensington lock (anti-theft control) when left unattended, for example locked to a desk within Company premises and offsite locations. When travelling or working off site, the user is responsible for ensuring that their laptop is secure and must take appropriate measures for protecting their laptop from loss, theft or damage
- h. When using your laptop or mobile devices in public areas, for example in airports, you should be aware of “shoulder surfing” when other people may be able to view your screen contents. If Protected Information/ Data are likely to be displayed, then you must ensure that this information is not visible to others. To achieve this, you could use an appropriate screen privacy filter which can be procured using a Service Request for “030 - Equipment & Accessories” then “010 - Supply Accessory”. Users should avoid viewing sensitive information and discussing confidential matters in public areas, and must ensure that such information and discussions remain private
- i. You may not have personal parcels delivered to any ScottishPower site.

3.2.3. Use of Equipment not Owned by ScottishPower

Most individuals own one or more items of personal Equipment in the form of mobile phones, smart watches or tablets. Although you may bring these to work with you, there are restrictions on how and where these may be used in the workplace. Equally, a third party may need to transfer information from their removable media as part of their work with ScottishPower. This section summarises the guidelines and requirements as set out in the Rules. Please be aware of the following and if you need more information, refer to the related Rule/s and/or your manager:

- a. Under no circumstances may you connect any device not owned by ScottishPower to the Company Cyber-Infrastructure without specific and advance authorisation from Cyber Security UK
- b. Should there be a need for a third party owned device to be connected to the ScottishPower Cyber-Infrastructure, you must obtain prior approval from Cyber Security UK
- c. You must never store or transfer any ScottishPower Protected Information/ Data onto Storage Media not owned by ScottishPower
- d. In accordance with the Data Extract and Handling Rule, under no circumstances may any Storage Media be shared between third parties and ScottishPower without prior written authorisation by Cyber Security UK, before being connected to the ScottishPower Cyber-Infrastructure
- e. Subject to local business requirements, mobile telephones should not be brought into areas of the business dealing with Personal Data (including, but not limited to employee and customer data), unless supplied by the Company for official business purposes
- f. If you are required to make or take a personal call using your personal mobile telephone during working hours, these calls should be made or taken away from work stations and work areas
- g. Personal calls during working hours must not be excessive or impact on daily work activities
- h. The use of personal Equipment within working areas is strictly prohibited
- i. If you have a requirement to use a personal device for mobility, please contact Cyber Security UK for guidance and formal approval.

Failure to comply with the rules and requirements above and those highlighted in section 5.3 may result in action under the Company’s Disciplinary procedure.

3.2.4. Misuse of Electronic Communications and Equipment

For the purposes of this Policy, “misuse” of the Company’s Electronic Communications and Equipment is defined as any use of Equipment where the usage:

- a. Has the potential to have a detrimental impact on the confidentiality, integrity or availability of the Company’s Cyber Assets
- b. Has the potential to damage any aspect of the Company’s Cyber-Infrastructure
- c. Could lead to or assist with illegal activity
- d. Risks legal liability to the Company
- e. Has the potential to damage the reputation of ScottishPower
- f. Breaches any of the clauses laid out in this Policy or any other of the Company’s Rules



- g. Breaches the Company's Code of Ethics (that can be found on the Company Intranet portal) or any other relevant Rules
- h. Breaches any legislation or associated code of practice
- i. Involves unauthorised access of IT systems, including your own energy account or the energy account of friends, family or colleagues
- j. Would involve enabling the hotspot or tethering options on ScottishPower mobile devices as these can cause excessive communications charges, should you have such a requirement please contact General Services, Mobile Phone team for guidance or refer to the Mobile Phone Policy on the intranet.
- k. May cause damage to Equipment.

For further information please refer to Guidelines for Personal Account Management which are found on the Intranet Portal. Also, please see the Reporting section of this document.

3.2.5. Storage Media

It is easy to inadvertently use Storage Media in breach of the clauses of one or more Rules, hereafter follows a summary of the correct usage of Storage Media within the Company:

- a. Only Company issued and approved Storage Media is allowed to be used
- b. All Storage Media must be acquired using the formal ScottishPower Service Request system
- c. You are responsible for ensuring that only ScottishPower approved Removable Media is connected to ScottishPower Equipment. Please contact Cyber Security UK if there is a need for connection by a non-Company standard (or externally provided) USB Device
- d. You may not copy Protected Information/ Data to Storage Media without prior authorisation from Cyber Security UK
- e. Company issued Storage Media is assigned to the individual and uses the correct level of encryption. You shall not disable or attempt to bypass or defeat this encryption in any way
- f. Storage Media should never be sent in the (physical) mail. If you need to send Protected Information/ Data to anyone outside of the ScottishPower Cyber-Infrastructure, please contact Cyber Security UK for guidance
- g. Please be aware that you must be able to provide an audit trail of data you have received and handed over including signatures and other evidence of handover, in line with the Rule.

If you have any doubt or questions relating to data handling, please ask your line manager or Corporate Security for guidance.

Failure to comply with the rules and requirements above and those highlighted in section 5.3 may result in action under the Company's Disciplinary procedure.

3.2.6. Use of Equipment/Data Offsite

You may be required to use ScottishPower Equipment or process data offsite away from ScottishPower premises. In these circumstances, extra care must be taken to ensure the protection of ScottishPower Equipment and Protected Information/ Data. There are a number of Rules mentioned at the end of this document that give the requirement specifics, however, the following is a list of the most important points. If you are in doubt about any of these requirements, you should discuss your specific requirement with your line manager to ensure that you are able to comply with the Rule/s.

- a. ScottishPower Equipment or Protected Information/ Data offsite:
 - i. Adequate security precautions must be observed whenever ScottishPower Protected Information/ Data is held or processed offsite from ScottishPower premises
 - ii. If a laptop is lost or stolen, this should be reported immediately to the Service Desk and to the Cyber Security UK mailbox
 - iii. Equipment must never be left unattended unless locked (password protected) and must be stored securely when not in use
 - iv. Be aware that with laptops and other devices are delicate and susceptible to damage by rough handling, theft or extreme temperatures. Users are responsible for their Company portable devices; these can easily be stolen or lost, so should be kept with you at all times. When travelling, you must always carry your laptop as hand luggage and never check it in as hold baggage



- v. Should there be a legitimate business requirement to record customer telephone transactions, recordings of customer telephone transactions must never be copied to Storage Media nor be taken offsite without specific authorisation. Also bear in mind that recording conversations has legal and other ramifications and you should discuss this with your line manager for prior authorisation
 - vi. Personal Data (including, but not limited to employee and customer data) must never be taken or sent off site, using any method, without specific prior written authorisation. Should there be a legitimate business requirement to transfer data, you should discuss this with your line manager for authorisation in the first instance.
- b. Storage of Protected Information/ Data on Portable Devices:
- i. If you have been provided with a Portable Device for business purposes, be aware that these are more vulnerable to theft and you must therefore take extra care to ensure that the devices and data stored on them are secure
 - ii. Where there is a business necessity to store Protected Information/ Data on a Portable Device, prior written consent must be obtained from your line manager and you must make sure that the data is stored using the right level of encryption. Please remove any information immediately when you no longer require it
 - iii. Personal Data stored on Portable Devices must be kept to a minimum, must be stored in encrypted form and should be deleted when no longer required. Users must adhere to the Information Management Rule
 - iv. Users saving Personal Data to Portable Devices will accept responsibility for being able to identify exactly what is saved on the device at any time and be able to produce an exact copy, if required. They must also be able to produce the relevant prior written authorisation if required
 - v. Users should not retain master documents of Protected Information/ Data on Portable Devices, where possible. Master and sensitive documents should be saved within a secure shared area to ensure it is backed up in the event of loss or theft.
- c. Storage of Company Confidential Information on Portable Devices:
- i. Where there is a business necessity to store Company Protected Information/ Data other than Personal Data, no authorisation is required. However, users are responsible for only having such information stored on the device where there is a current business necessity. Such information must be encrypted and users are responsible for knowing what is stored.

If you have any doubt or questions relating to data handling, please ask your line manager or Corporate Security for guidance.

Failure to comply with the rules and requirements above and those highlighted in section 5.3 may result in action under the Company's Disciplinary procedure.

3.2.7. Data Protection

The General Data Protection Regulation (GDPR) sets out a framework for the protection of Personal Data regarding Staff, customers, suppliers and other individuals used by the Company for a variety of purposes. When handling or processing Personal Data, there are strict legal requirements which must be adhered to, failure to do so could cause ScottishPower to be fined. All Users are responsible for complying with the GDPR principles and must be able to demonstrate compliance at all times. The most relevant ScottishPower Rule relating to GDPR is the Information Management Rule; the following are the salient points:

- a. Working with Personal Data must be done according to strict guidelines that dictate how information may be; collected, processed, relevant to the purpose it is being used for, retained, kept secure and maintained
- b. When Personal Data is being processed, the basic principle is, because the information is likely to be of a private nature, it needs to be treated with greater care than other data
- c. All individuals have enhanced rights over their Personal Data, including rights to; access a copy of their data, have inaccuracies rectified, or even erased under certain circumstances
- d. If Personal Data is accidentally or otherwise destroyed, lost, altered, disclosed or accessed, this must be reported to the DP&P team as soon as possible
- e. You will be required to complete a mandatory GDPR training course.

There are many more aspects to the GDPR which all Staff must comply with when handling or processing Personal Data. To implement the requirements of the GDPR, ScottishPower has a Data Privacy & Protection (DP&P) team as well as DP Managers in each business. If you are in doubt about any aspect of the GDPR, you should contact your line manager or the Data Protection Manager for your business to ensure that you are able to comply with the GDPR.



You should be aware that if you fail to comply with the rules and requirements above, this will be considered a serious breach of this Policy and you may be subject to disciplinary action, which could result in the termination of your employment.

3.2.8. Data Classification, Handling and Transfer; Rules and Requirements

Users must take care to protect Company Protected Information/ Data, especially when transferring information. If you need to work with or transfer ScottishPower data then you must familiarise yourself fully with the Rules listed at the end of this section. Notwithstanding the extent of the GDPR, hereafter follows a list of the salient points from the Rules that are worth keeping in mind when working with ScottishPower data:

Data Classification

The Information Protection User Guide specifies how to correctly classify the information you work with and you are encouraged to be aware of the full rule contents. The following is a summary of the more pertinent points from the Rule:

- a. All Information/data has to be classified based on the ScottishPower Information Classification and Protective Marking Standard
- b. Documents must carry a classification marking within the document header or footer of each page, clearly stating the classification of the document
- c. The information/data custodian is responsible for protecting data in accordance with ScottishPower policy, rules, applicable regulations, laws and the Information/data owner's specific requirements.

Data Extract and Handling

Data transfer brings a risk that ScottishPower Protected Information/ Data might be lost, misappropriated or accidentally released. It is the responsibility of the ScottishPower user (the requester of the extract) to assess all risks and ensure that adequate controls are in place for compliance with this Policy. This section contains examples that must be considered before transferring information, but is not exhaustive. Guidance should be sought from Cyber Security UK should alternate methods of transfer be considered.

Secure Transfer by Email

Email is not a secure way of transferring information; this section gives you some pointers about safely transferring information via email:

- a. Data stored on Equipment and Storage Media throughout ScottishPower contains propriety information as well as confidential and sensitive information
- b. Where data is transferred by email, this should be used only for Extracts that (when encrypted) are of a small size, the email system limits transfers to a maximum of 5MB, larger attachments should be done using Electronic File Transfer as below
- c. Where any Protected Information/ Data and in particular Personal Data must be transferred, email transfer should NOT be used. In this case, the data should be stored in an encrypted file, such as a password protected ZIP file, which is then transferred using the approved Electronic File Transfer mechanism
- d. Any password to open the attached file must be transferred to the recipient using a different method than email, e.g. a telephone call to an agreed telephone number, a closed letter or an SMS message.

Electronic File Transfer

- a. Standard approved file transfer methods are made available to authorised users on a limited basis. Systems such as Serafin or ShareFile ensure the minimum level of security is met
- b. Users must only transfer ScottishPower Protected Information/ Data by the means of the approved file transfer mechanisms and such information may NOT be transferred by email
- c. Only ScottishPower employees may conduct file transfers.

This includes information (data) protected by national or international security and privacy regulations and standards as well as data protected by confidentiality agreements.

Failure to comply with the rules and requirements above and those highlighted in section 5.3 may result in action under the Company's Disciplinary procedure.



3.2.9. Disposal of Digital Records

Data stored on computer systems and electronic media throughout ScottishPower contains propriety information as well as confidential and sensitive information. To prevent unauthorised access to this information, all Equipment and Storage Media must be properly cleaned of sensitive information and software before being transferred outside of ScottishPower either as surplus equipment or as waste.

Types of disposal and their applications have been listed below:

- a. **Shredding** – Used for disposal of paper, CDs and DVDs
- b. **Purging** – Used for disposing Storage Media such as hard disks, digital tapes etc. by pulverisation, drilling, melting/incineration. These types of media should be passed to IT for correct disposal
- c. **Disk Wiping/File Shredding** – For situations where the media must be retained for future use, but the data must be wiped off it. This method is best suited for USB memory sticks, Portable Devices and desktop hard drives where the equipment is to be reused, contact IT for assistance.

Failure to comply with the rules and requirements above and those highlighted in section 5.3 may result in action under the Company's Disciplinary procedure.

3.2.10. Clear Desk and Device Screen

To prevent the compromise of the confidentiality, integrity and availability of ScottishPower data and electronic equipment there is a Clear Desk Rule that specifies how Users should leave their working space when they leave the office. A summary of the Rule requirements is captured here, but users are urged to familiarise themselves with the full detail of the Rule to ensure that they can comply fully. Users shall take steps to ensure a clear desk, screen and workplace by:

- a. Locking away business critical and/or sensitive information, e.g. on paper or on Storage Media, when not required (or not in use)
- b. Shredding business critical and/or sensitive documentation when no longer needed, consistent with ScottishPower's record retention and destruction policies
- c. Logging off or protecting computing resources (desktops, Portable Devices, terminals, etc.) with a screen and/or keyboard locking mechanism, controlled by a password, token, or combination of user authentication mechanisms when unattended or when not in use. To prevent others accessing your workstation, use <Ctrl><Alt><Delete> together on your keyboard and select "Lock Computer" or press <Windows-key> + L together
- d. Use photocopiers and other reproduction technology (e.g. scanners, digital cameras) only when necessary and when authorised to do so. Please remember to retrieve the originals and any printouts from these devices when finished
- e. Please remember not to leave any Storage Media containing Protected Information/ Data in conference/ meeting rooms when you leave them.

Failure to comply with the rules and requirements above and those highlighted in section 5.3 may result in action under the Company's Disciplinary procedure.

3.2.11. Limited and Reasonable Personal Use

The Company operates its Cyber-Infrastructure for business related purposes, although it is recognised that you may on occasion use Company resources in relation to personal matters.

- a. You must not under any circumstance use a Non-Company issued SIM (e.g. a personal SIM) with a Company issued device
- b. You may not under any circumstance use a Company issued phone SIM in a non-Company owned mobile phone
- c. Use of both Personal as well as Company issued mobile devices must be in accordance with the provisions of the Mobile Phone Policy.

Personal Use of Electronic Equipment

Use of the Company Cyber-Infrastructure and electronic communications resources includes but is not limited to all the Equipment as defined in the Definitions section

Personal usage must:

- a. Be kept to a minimum



- b. Be limited to reasonable personal use
- c. Not be used for social “chat or networking” for example using email to have a non-work-related conversation, your ScottishPower email address is for business use only
- d. Be used on an “occasional basis”, preferably outside of normal working hours or during break times
- e. Be kept brief, for example when sending emails
- f. Not include large attachments such as photographs, music or video files
- g. Never cause the Company to breach legislation or other obligations
- h. Never contain Offensive or Defamatory Material (as defined in the section “Offensive or Defamatory Material”) or otherwise, which could potentially cause offence or embarrassment to customers, colleagues or managers
- i. Never contain material which infringes third party copyright or other intellectual property rights
- j. Never impact on your productivity or ability to meet work targets, deadlines or objectives
- k. Never be used in connection with any other business activity not related to ScottishPower
- l. Never be used for private commercial activity, gambling or any other form of personal gain
- m. Avoid using your Company email address for anything other than for business purposes
- n. Never use your Company email address to subscribe to any non-business-related newsletters, mailing lists or news groups as this wastes time and resources.

Limited and Reasonable Use

The term “Limited and Reasonable Use” may be open to interpretation, so you are responsible for ensuring that your level of personal use does not exceed what the Company would reasonably regard as an acceptable level.

When considering whether your level of personal use is limited and reasonable, ask yourself:

- a. Do you spend significant amounts of your time using Company resources for personal matters?
- b. Do you send a lot of non-business-related emails?
- c. Could your usage be considered excessive by others?
- d. Does your level of personal use ever impact on the quality of your work performance?
- e. Does your level of personal use mean that you sometimes don’t meet your work targets, deadlines or objectives?
- f. Could you be more efficient and productive, if you were to spend less time sending personal communications or using Company resources for personal matters?
- g. Would you be embarrassed to tell your line manager about the amount of time you spend sending personal communications or using Company resources for personal use?
- h. Would the material you are downloading, viewing or sending be a breach of relevant legislation on copyright, defamation or misuse of computers or any other applicable laws?
- i. Do you use Company resources in connection with any external business activity on behalf of yourself, a family member or friend, club or charity?

If the answer to any of these questions is “yes”, then it is likely that you are breaching what the Company would regard as acceptable limited and reasonable personal use.

Use of the Company Cyber-Infrastructure for personal reasons is a privilege that may be withdrawn at any time. **You should be aware that if the Company considers your level of personal use to be unacceptably high, you may be subject to disciplinary action, which could result in the termination of your employment.** For the avoidance of any doubt, the Company shall be the sole determiner of what constitutes “Limited and Reasonable Use”. If you are unclear about what constitutes “Limited and Reasonable Use”, you should discuss this with your line manager.

3.2.12. Offensive or Defamatory Material

For the purposes of this document, the term “Offensive or Defamatory Material” is defined as any Electronic Communication that the Company considers to be:

- a. Discriminatory (including but not limited to age, disability, race, religion or belief, sex, gender identity, sexual orientation, marriage and/or civil partnership, pregnancy and maternity)



- b. A breach of Equal Opportunities legislation
- c. Pornographic, paedophilic, sexually explicit or otherwise obscene or offensive
- d. Abusive, threatening, intimidating, hostile or otherwise inappropriate language
- e. A threat or personal attack made against any individual or corporate body
- f. Harassing, bullying, or humiliating
- g. Libellous, defamatory or derogatory
- h. The other party may reasonably consider as offensive or take offence at
- i. Unlawful under UK law (Scotland, England, Wales and Northern Ireland), the laws of any destination country, or any country via which such material travels to reach its destination.

The content that you download, view or send using Company resources is your decision, based on the guidance in this policy. When using Company resources, you should ask yourself:

- Could the material being downloaded, viewed or sent, cause offence or embarrassment if customers, colleagues or managers were aware of the content?
- Would you be embarrassed or uncomfortable, if an email was read aloud or any image was held up at a Disciplinary Hearing, Court or Tribunal as part of Legal proceedings?

If the answer is “yes” to either of these points, it is likely that it could be considered to be Offensive or Defamatory Material. If you are still unclear about what constitutes Offensive or Defamatory Material, you should discuss this with your line manager.

You should be aware that if you use Company Equipment to create, obtain, transmit or otherwise handle Offensive or Defamatory Material, this will be considered a serious breach of this Policy and you may be subject to disciplinary action, which could result in the termination of your employment. For the avoidance of any doubt, the Company shall be the sole determiner of what constitutes Offensive or Defamatory Material.

3.3. Access Control

Protection of ScottishPower’s Cyber-Infrastructure is driven by business, legal, regulatory, financial and operational requirements. This section identifies a set of requirements the users must adhere to in order to develop a framework and plan to manage Cyber Assets based on their levels of sensitivity, value and criticality to ScottishPower.

3.3.1. Access Management Requirements

ScottishPower implements physical and logical access controls across its Cyber-Infrastructure in order to provide authorised, granular, auditable and appropriate user access, and to ensure appropriate preservation of data confidentiality, integrity and availability in accordance with the Information Security Rules. To maintain effective security, it is vital to ensure that data can only be accessed and processed by authorised users. Access management is used to detect and prevent unauthorised access to ScottishPower’s Cyber-Infrastructure and Protected Information/ Data.

The Access Governance Rule specifies the full detail of all requirements for managing ScottishPower’s assets and data, a summary of some of the most important requirements follows, but please ensure you refer to the Rule for the full detail:

- a. Both logical access and physical access shall be taken into consideration when granting access to the Cyber-Infrastructure
- b. Before access to ScottishPower Information Systems is granted, formal authorisation must be obtained
- c. Authorisation is obtained by using the Service Request process, found under “IT Requests and Incidents” in “My Corporate Applications”. The Service Request process is used for requesting, authorising, granting, reviewing and revoking access rights for all Users and ensures appropriate local authorisation (based on a user’s Department) and authorisation by the System Owner
- d. Only Users with a legitimate business need to access systems and data should be given access rights on a need-to-use basis and/or on an event-by event basis based on the minimum requirement for their functional roles. When access is no longer required, for example when an User changes role or leaves the Company, access privileges should be revoked
- e. Managers shall not log in as the new user when they receive the user’s logon information to request access, this must be done by the new user



- f. ScottishPower will provide Users with access to the Information/data they need to carry out their responsibilities in as effective and efficient a manner as possible
- g. Line managers / System owners are responsible for ensuring that access control is correctly established for all Users and entities within the ScottishPower Cyber-Infrastructure. Line managers control access (local authorisation) to information systems and networks for their direct reports. Line managers and System owners must:
 - i. Strictly control access to ScottishPower systems
 - ii. Review access rights at least once annually
 - iii. Review and adjust (via Service Request) User's access rights after any changes in their function including promotion, demotion and re-allocation from role to another within ScottishPower
 - iv. Ensure that the appropriate request is raised to revoke system access/shared access privileges immediately upon the User leaving the organisation.

Failure to comply with the rules and requirements above and those highlighted in section 5.3 may result in action under the Company's Disciplinary procedure.

3.3.2. Users Changing Role or Leaving

When users change role or department, line managers must raise a Service Request to revoke/amend the individual's system access, including shared access areas. Managers must also check that requests have been actioned. The following must be kept in mind:

- a. The access rights of all Users of the ScottishPower Cyber-Infrastructure must be removed upon termination of their employment, contract or agreement, or adjusted upon change of employment
- b. Managers must lodge the necessary request to remove a leavers access within 24 hours.
- c. User systems /shared area access should be reviewed regularly by line managers and system access levels updated to ensure that users have the correct level of access for their respective role
- d. Users should not retain system access/shared area access when changing role, unless it has been specifically identified as required and approved by their new line manager. Line managers should also ensure that Your HR On-line is updated to reflect the change of role/department/manager
- e. Both the User's existing and the new line manager should discuss and agree system access/shared area access privileges before raising service requests for Users. It would be operationally impractical to revoke a User's access when changing role, if systems/shared area access is still required for the User's new role
- f. Following completion of business approval for system access, as a User you should be aware that you can install, and subsequently de-install applications which are no longer required, by loading the Corporate Applications Installer, browse to the application, double click and select the "install this product" button or the "uninstall this product" button. If you experience difficulties or require guidance, you should contact the Service Desk
- g. The User's existing line manager is responsible for ensuring that systems access/shared area access privileges have been revoked prior to the User leaving their responsibility
- h. The User's new line manager is responsible for ensuring new systems access/shared area access privileges are created as dictated by job function. The new line manager is responsible for ensuring the provision of only such access as required to fulfil the requirements of the managed user's new role
- i. When a User leaves the Company, the line manager should follow HR procedures for leavers when conducting the exit interview with the User and raise a Service Request within 1 working day to revoke the User's access rights
- j. The line manager is responsible for ensuring that HR is updated with the exit interview and that the Asset Return Checklist has been completed
- k. Line managers must ensure that all Company assets, Equipment and Security pass are returned.

Further information and guidelines for leavers can be found on the HR intranet under "Leaving the Company".

Any unnecessary access levels afforded to Users after they are no longer the responsibility of their manager may constitute a breach of the UK HR Security Rule and could subject the previous line manager to disciplinary action, which could result in the termination of their employment.



For the avoidance of doubt, where the line manager is not an employee, responsibility falls to the individual moving up the organisational hierarchy until such times as the individual is an employee.

3.3.3. Logins and Passwords/Passphrases

- a. The primary access control mechanism for accessing ScottishPower Electronic Communications Equipment (for example personal computers, laptops and computer applications), is via a login and password system.
- b. You should note that the use of login identifiers and passwords is required to control access to ScottishPower systems and data on a strictly need to know basis, relevant to job function. This simple but highly effective protection is rendered useless if passwords are shared or workstations are not locked when left unattended.
- c. Managers with authority to grant access rights to a user or group of users should consider the following:
 - i. Need for access
 - ii. Potential conflict with segregation of duties
 - iii. Business separation requirements
 - iv. Incompatible job functions
 - v. Level of access required (read, update, delete)
 - vi. Period of access required.

The sharing of logins and passwords is strictly forbidden and may result in disciplinary action, which could result in the termination of an individual's employment. Managers who knowingly approve or condone the practice of sharing logins and passwords may also be subject to disciplinary action, which could result in the termination of their employment. ScottishPower operates a zero-tolerance policy on the practice of sharing logins and passwords.

3.3.4. Choosing a Password

As users of the Company Electronic Communication systems, you are provided with an individual account accessed by a unique user ID and password. In order to prevent unauthorised access, users are required to keep their password secret and must never disclose their password to anyone else. If you suspect that someone else knows your password you should change your passwords (press <Ctrl><Alt><Delete> and select Change Password).

- a. A good practice in forming passwords is to use passphrases rather than just a password. As a general rule, passwords should be strong, complex and made up with special characters (i.e. '!"\$%^&*()@~#') in most cases and using passphrases is the easiest way to achieve this. Some considerations about how you form your passwords:
 - i. Using passphrases helps generate long and complex passwords that are not predictable, yet are easy to remember and type. Passphrases should be long enough to be hard to guess and not be recognisable from literature, holy books, poetry, the movies, slogans etc. They should be hard to guess, even by someone who knows the user well. For example, "H1reda*Mustang5.0*inOrlando!" is easy to remember, contains many special characters and is long, so would make a good password
 - ii. A different approach is to use a sentence to deliver a password, so "I went on holiday to Florida with a 5.0 Ford" could be used to remember a password "Iwoh2Fwa5.0f", also a long password that contains special characters
 - iii. As a general rule, the longer and more complex the password, the less likely it is to be cracked.
- b. For mobile devices, there are many authentication options and also options on what the device will do in the event of authentication failures, including locking the device or erasing its contents. Please check the Mobility Rule and contact Cyber Security UK for guidance on the best settings to make for your requirements. Specifically:
 - i. If your device uses fingerprint recognition, you should register more than one finger to make it easier to use if you want to swap hands or if you have damaged your finger
 - ii. Depending on local rules and procedures, the device may be remotely tracked, disabled or wiped
 - iii. Users granted use of a ScottishPower mobile device must participate in any required local mobile device awareness training.



3.3.5. Password Policy

You must comply with the Company Password Policy, for further guidance see the Access Governance Rule. Password requirements vary in nature and requirement from system to system, where some require passphrases or pin numbers, others need a user ID and password for authentication. For systems requiring a user ID and password, passwords are required to be changed periodically and, when you have to, will typically show a window with the specific password requirements for the given system. Please review these carefully, as they may change as security requirements evolve.

You should change passwords regularly, use passphrases to keep them long and complex and store your passwords safely using a secure password store; and also heed the following recommendations:

- i. The Rule is clear that security and passwords must not be defeated or bypassed on any system
- ii. Passwords/ passphrases must not be reused between sites, applications and other locations like internet sites or mobile apps
- iii. Keep passwords confidential - they should never be shared or revealed to anyone
- iv. Passwords must not be written on paper or electronically stored in unencrypted form
- v. If you have access to company email, you can store passwords in an Outlook Note in your personal mailbox. Passwords must not be stored within a shared mailbox, as they would be visible to other mailbox users with access
- vi. Change passwords whenever there is any indication of possible system or password compromise, for example when a member of a work group leaves the Company, the work group password should be changed
- vii. For a subset of systems, the Company has implemented password management tools which will synchronise user names and passwords. Password management is suitable for application passwords which are linked to your network account and may be also used for saving passwords for other systems and applications.

Note that on some systems your user account will lock out after a number of failed login attempts. If you did not cause any login failures, but have been locked out, you should notify the Service Desk immediately.

Weak Passwords

Some examples of the types of passwords that are considered weak, easily guessed or broken are:

- Names, initials, payroll numbers, telephone numbers, car registration numbers, Mother's maiden name, Children's name, Pet names
- Spouse, partner or children dates of birth
- Passwords set to "password"
- Passwords with two or more consecutive identical characters
- Well known phrases
- Dictionary words.

Failure to comply with the rules and requirements above and those highlighted in section 5.3 may result in action under the Company's Disciplinary procedure.

3.3.6. New IT Systems

ScottishPower has rules and procurement processes to control the introduction of new IT services in any part of the organisation. For full details, please refer to the Rules below, however, the following is a summary of the most important aspects of these Rules:

- a. You may not use any personal or other non-Company IT equipment for processing business information
- b. You must always use the correct procurement process to acquire Storage Media, don't use media you bring in, you will be infringing one or more Rules
- c. New IT capability or services must have the appropriate management approval, authorising their purpose and use
- d. Approvals may be needed from Cyber Security UK to ensure that an appropriate risk assessment has been performed assist to ensure the appropriate control requirements are in place
- e. When acquiring, developing and maintaining a system or solution you must refer to the Asset Acquisition, Development and Maintenance Rule to ensure a secure environment within ScottishPower.



Failure to comply with the rules and requirements above and those highlighted in section 5.3 may result in action under the Company's Disciplinary procedure.

3.4. Electronic Communication Tools

The Company electronic communications systems are made up of a number of different types of service; Email, Instant Messaging and Collaboration Networks. These are tools for gathering and distributing information to individuals or groups quickly and accurately.

- Email is best suited for the sending and receiving of specific information, for example text documents, spreadsheets, presentations and other documents to multiple recipients
- Instant Messaging is more suited to brief conversations, consisting of short questions, answers and comments
- Collaboration Networks are ideal for team discussions, cross-group input, sharing updates, gathering ideas and reaching decisions.

The Company encourages you to consider what will be the most effective means of communication on a particular matter. Where the topic is a sensitive matter, has political impact or is otherwise a complex or a confidential matter, a phone call or a face-to-face discussion is often a better way of communicating. Improper use of electronic communication tools can result in miscommunication, tension and conflict between Users, which reduces overall productivity and may contribute to a negative working environment

Company resources should only be used for legitimate business purposes. When accessing electronic communication systems, you should be aware that such usage is routinely monitored by ScottishPower. By accessing any Company systems, you are deemed to have consented to system monitoring without further notification.

3.4.1. Instant Messaging Rules and Best Practice

With the exception of Skype for Business, communication via Instant Messaging is prohibited. Skype for Business is available to users where required and formally approved. You should be aware that messages (including text messages) may be recorded and will be treated in the same way as emails. When using Skype for Business:

- a. Personal Data must never be transferred or displayed when sharing your screen
- b. In your communications, it is good practice to use proper language and to avoid using abbreviations, shortened phrases, acronyms and "text-ese" because these can be misinterpreted, with negative results
- c. It is good practice to re-read each message for accuracy, spelling and to verify that the recipient address is correct before sending it; as most messages cannot be recalled once delivered
- d. To ensure the ongoing safe and efficient operation of the Company Instant Messaging systems, please ensure that you:
 - i. Check that you will not be transmitting Protected Information/ Data, if you are, contact Cyber Security UK for guidance on how to send confidential or restricted information
 - ii. If you need to transmit Protected Information/ Data or other sensitive information to colleagues, you should explore whether this can rather be done through secure file transfer
 - iii. You must always send the minimum amount of information possible to fulfil your purpose and each recipient must only receive the information they need.
- d. Instant Messaging shall not be used for transmitting, retrieving or storing any messages, files or attachments which might infringe (but not limited to) any of the following:
 - i. Advertising, spam, politics, sex or religion
 - ii. Harassing, defamatory or discriminatory messages
 - iii. Messages that violate copyright, trademark, or other intellectual property rights
 - iv. Obscene or offensive materials
 - v. Messages in breach of applicable laws, regulations or other ScottishPower policies
 - vi. Passwords or other confidential information.



3.4.2. Collaboration Network Rules and Best Practice

ScottishPower provides Collaboration Networks such as Microsoft Yammer and Microsoft Teams internally on a limited and restricted basis. For both of these facilities, there will be separate codes of use and governance models. When using any collaboration tool, the same Rules and Best Practices as Instant Messaging in the previous point apply, with the following additional recommendations:

- a. To avoid wasting time, when starting a collaboration, only include contributors who have a direct need to be involved
- b. If the collaboration has resulted in a decision, follow this up with a confirmation email to the contributors, because the discussion history may not be available for reference in the future
- c. Try to avoid topics of a very complex, political, contentious, personal or confidential nature, as this may not be the best communications platform for these types of discussion
- d. If you give your opinion, it is important to distinguish between the personal and the professional when representing your department or business area
- e. Should you have any doubts regarding the appropriateness of what you intend to publish, it is better not to submit it
- f. GIFs and emojis are useful on some occasions to help emphasise a comment, however, overuse may produce the opposite effect.

3.4.3. Email Usage Rules and Requirements

Email is perceived to be less formal than paper-based communication and there is a tendency to be casual about message content. However, emails are used for business correspondence and what you write should be accurate and professional. You could be held accountable for what you send and so you should always remember that expressions of fact, intention and opinion via email may be used in the same way that verbal and written statements could be used against yourself or ScottishPower.

Most Users are provided with access to the Company's email system, which is a major communication channel for the business. Acceptable use of email includes the following:

- a. Company email accounts are only intended to support legitimate professional requirement to fulfil your responsibilities
- b. The use of personal devices (non-Company owned or provided) for company email is strictly prohibited. This would result in Company data being stored on a non-Company owned devices, which is an unacceptable risk
- c. Only Company email addresses should be used for business communication. Personal email addresses should not be used under any circumstances for ScottishPower business correspondence. Similarly, Third Party contractors should only use their business email addresses for correspondence on ScottishPower's behalf, which will help to ensure that appropriate security controls are in place
- d. Do not send Company Protected Information/ Data via email
- e. Sending Company Protected Information/ Data from your ScottishPower email account to personal/home email accounts is prohibited
- f. If you are required to access business emails from home, you should raise a Service Request for remote access, or use Outlook Web Access (OWA)
- g. When you use Outlook Web Access (OWA) to access your email, you must be extremely careful not to retrieve sensitive information or files from non- Company equipment, as temporary files may leave data on the machine. Users are responsible for ensuring that temporary files are deleted
- h. Your Email and signature should comply with ScottishPower corporate branding, including but not limited to use of font, corporate logos and images
- i. Users must not spoof by forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any ScottishPower electronic communication to mislead the recipient about the identity of the sender
- j. Subscribing to non-work related mailing lists, newsgroups, newsletters etc. using your ScottishPower email address is prohibited
- k. ScottishPower does not classify email systems as a document storage mechanism, but rather as a communication tool. Subsequently, the Company has an email retention policy that specifies the removal of all messages older than a certain time (presently 18 months), to prevent storage and capacity issues.



Therefore, please ensure that you store important messages and attachments that need to be retained to corporate storage spaces and network resources

- I. Limited use of ScottishPower Email facilities for personal purposes shall be regarded as acceptable provided that:
 - i. Messages are not used for private professional (business) or other commercial purposes, including the sale or purchase of goods or services,
 - ii. Use does not interfere with the normal performance of the User's duties,
 - iii. There is no breach of the prohibitions identified in the Rules.

Misuse of email and in particular unprofessional, inappropriate language or email content which are detrimental to ScottishPower's reputation and business are not acceptable and may result in disciplinary action, which could result in the termination of your employment. For the avoidance of any doubt, the Company shall be the sole determiner of what constitutes misuse, unprofessional, inappropriate language and excessive use of email.

3.4.4. Prohibited Use of Email

As with other modes of communication, when dealing with third parties on the Internet, you are required to observe the Rules. **Please be aware that the following activities are strictly prohibited and engaging in such activities when using email may result in disciplinary action, which could result in the termination of your employment.** For the avoidance of any doubt, the Company shall be the sole determiner of what constitutes misuse, unprofessional and excessive use of email.

When using email, you should:

- a. Never send excessive amounts of personal emails in excess of limited and reasonable personal usage guidelines
- b. Not encourage activities which make unproductive use of your and colleagues time or that promotes activities which would be illegal or unlawful
- c. Not partake in activities outside the scope of your responsibilities, for example unauthorised selling/ advertising of goods and services
- d. Never send or forward "junk", "chain", "spam" or "hoax" email. "Junk" or "chain" mail as this slows down the system for all Users and is expensive and time-consuming to remove
- e. Avoid messages that may damage, overload or adversely affect the performance of ScottishPower's Cyber-Infrastructure and/or external communications in any way
- f. Never use email like "chat", there are dedicated systems for that
- g. Never send or forward email attachments if you cannot verify the contents. If you receive an email with an attachment which you suspect may contain unsuitable material, unsubscribe from the site (if the option exists), delete the email and reply to the sender instructing them not to send you any similar material. If they persist in sending you inappropriate emails and/or attachments, you should contact your line manager for advice
- h. If you receive an email with an attachment which you suspect may contain an attempt at phishing (tricking you into providing personal data or login information), do not click on any links contained in the message and use the PhishMe button on your toolbar. This will identify the message to IT for further research
- i. Use Reply-All only when it is important that all other recipients get your response. Using Reply-All as your default is not only wasteful of Company resources, but also wastes other's time
- j. Not send messages that may contain Offensive or Defamatory material or may otherwise be considered to be indecent or obscene. Equally, emails that might be offensive or abusive with contents that could be considered to be a personal attack, rude or personally critical, sexist, racist or generally distasteful
- k. Never bully or harass an individual
- l. Never breach Company Policy on Equal Opportunities
- m. Keep in mind that your attachments could infringe third party intellectual property rights, incur liability or otherwise impact ScottishPower.

Email messages, even those that have been deleted from the system, can be traced and retrieved and all persons having a part in creating or forwarding an offending email can be identified. Emails in both hard copy and electronic form, are admissible in disciplinary and legal proceedings.



Failure to comply with the rules and requirements above and those highlighted in section 5.3 may result in action under the Company's Disciplinary procedure.

3.4.5. Effective Use of Email

Hereafter follows a list of best practices and considerations you should take into account over and above the Rule:

- a. Check your email distribution list and only include those individuals with an absolute need to know. Use extreme caution when selecting email addresses from the address book, be aware that it is your responsibility to ensure that emails are sent only to the intended recipients
- b. In order to ensure the confidentiality of all parties, you must use the BCC field (Blind Carbon Copy) when sending email to distribution lists which contain email addresses of external parties
- c. Where regular emails are required, for example weekly reports, you should create an email distribution list to avoid distribution anomalies. However, you must take extreme care to select the correct email distribution list or you might inadvertently send the email to multiple users, including external parties, who have no authorisation to view the information
- d. Make appropriate use of the "Importance" and "Sensitivity" options when sending emails. Only use the "Urgent" flag for emails that are truly urgent in nature. Similarly, if something is less important the "Low Importance" flag can be utilised
- e. Only use the "read receipt" facility on messages for which you do actually require confirmation that the message has been received. The "read receipt" facility should not be used routinely nor as the default for all email correspondence
- f. When flagging emails for follow-up, only flag emails when they have been sent for your personal follow-up. Where emails have a timescale for response, this should be detailed within the email to ensure that recipients are aware of the timescale and priority required
- g. Use "Out of Office" replies if you are going to be out of office, detailing your return and alternative contact details for urgent requests. For external emails, to avoid social engineering and phishing calls, do not include your phone number in your signature. You can do this using templates in Outlook, for information on how to do this, contact Cyber Security UK for assistance
- h. Forward any emails received in error to the correct addressee (if identifiable) and notify sender
- i. Emails sent in error can sometimes be recalled, however this is not a guarantee the email won't be read prior to the recall. Users must ensure that immediate action is taken to recall emails sent in error
- j. Where emails are sent in error externally, users must escalate this to their line manager immediately to assess and minimise risk
- k. If you receive any Offensive or Defamatory material by email, report this immediately to your line manager
- l. Do not use backgrounds or "wallpaper" on your email messages.

Failure to comply with the rules and requirements above and those highlighted in section 5.3 may result in action under the Company's Disciplinary procedure.

3.4.6. Email Disclaimer

A standard email footer that includes a disclaimer message is added to the end of all external emails. This is to protect ScottishPower from unauthorised disclosure of information via this communication method. The disclaimer is added automatically as email leaves the ScottishPower infrastructure. For the avoidance of doubt the Company is the sole determiner of the email disclaimer content. No other form of disclaimer should be added to emails without prior written authority from Cyber Security UK.

3.5. Use of Company Internet and Intranet

Internet access is only provided to users who require the service to access information for business purposes. As a user of the Company's Cyber-Infrastructure, you do not automatically have access to the Internet. If you require Internet access this may be requested and granted subject to approval via the Service Request process.

If you are sponsored by the Company to undertake academic and professional qualifications, you are encouraged to use the Internet in the course of your studies.

3.5.1. Effective Use of Company Intranet & Internet

As a user of the Company's Cyber-Infrastructure, you have the ability to access the Company's intranet sites to read and print Company-wide information including announcements, policies and procedures, Company



reports and all other information displayed. Please keep in mind the following when accessing the Company Intranet and Internet:

- a. You must not forward any information from the Company's Cyber-Infrastructure to third parties without first obtaining approval from the Company
- b. If you download information from the Internet, you should bear in mind that because the Internet is unregulated, the information displayed on websites may be inaccurate or out of date. You should ensure that you check the reliability of the source before using downloaded information. There is also the potential risk of downloading virus, malware, Trojans and malicious software when accessing the Internet, you should take extra care when accessing and downloading information from the Internet
- c. You should be aware that the downloading, possession, distribution or copying of a copyright work, for example a document, photograph, piece of music or video, is an infringement of copyright unless the person downloading is properly authorised to do so by the copyright owner
- d. The Company accepts no responsibility or liability should you choose to use your personal credit or debit card to purchase goods or services over the Internet using the Company Cyber-Infrastructure. You should be aware that some websites are dangerous and include, for example hacking pages. You should ensure that when entering credit/debit card details, that the site you are accessing is secure (showing HTTPS:// in the address bar and a lock symbol). Heed all browser warnings!

Please be aware that misuse of the Internet, including spending excessive amounts of time using the Internet may result in disciplinary action, which could result in the termination of your employment.

3.5.2. Prohibited Use of Company Internet

- a. There are limited controls over what content individuals may decide to look at on the Internet. To protect Company resources and to reduce the likelihood of you being inadvertently exposed to Offensive or Defamatory Material (as defined previously in this document), access to certain websites, which the Company would consider to contain inappropriate material, is restricted by the use of Content Management Software. It is not possible to block access to all inappropriate content automatically; therefore, just because you are able to access a particular Internet location, you must not assume that the Company would consider it to be acceptable
- b. Should you inadvertently access a site which you suspect contain consider Offensive or Defamatory Material, you should close all your browser windows and notify your line manager immediately. Automated monitoring tools will record even inadvertent access of inappropriate content and this may result in further investigation. Keeping your line manager informed will ensure that matters are resolved promptly
- c. Most websites use cookies or other tags downloaded onto your computer to enable the site owner to identify and track visitors. This information could be a source of embarrassment, especially if inappropriate material has been accessed on the website. Such actions may be a breach of this Policy and Users should avoid accessing inappropriate content, even on legitimate websites
- d. The Company shall not be responsible or held liable for Offensive or Defamatory material which you might be subjected to whilst using the Internet from the Company's Cyber-Infrastructure.

The following activities are strictly prohibited when using the Internet through Company resources:

- a. Never try to subvert or bypass the Web Content Management software. If you believe you have a legitimate business need to access a site that is restricted by the Web Content Management Software, you should raise a Service Request for "010 - Grant Internet access"
- b. Never spend excessive amounts of time browsing or downloading material from the Internet
- c. Never access, receive, transmit, sell, purchase or download offensive or defamatory material
- d. Never access the Internet directly whether through a modem or through another Service Provider, unless the accessing computer is disconnected from all ScottishPower networks. Where a specific application requires a dial up modem, this should only be used for the specific application and with prior consent from Cyber Security UK
- e. When you are using a Company laptop offsite and are using a non-Company Wi-Fi, you should ensure that it is connected to the Cyber-Infrastructure using the Company secure VPN (Cisco AnyConnect) to protect the machine
- f. Never use external websites (e.g. Dropbox, Box, Google Drive, Microsoft OneDrive, WeTransfer etc.) for storing or sending Company Protected Information/ Data, as external storage exposes the Company to high risk with increased vulnerability



- g. Never abuse or misuse your Internet access for personal or business gain. Internet access is considered a privilege, which can be revoked at any time. Internet access is closely monitored by Internet Security and personal use should be limited and should not impact on work activities or targets
- h. Never download or install software from external sources without prior written authorisation from Cyber Security UK. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked before they are downloaded. If in doubt, you should contact the IT Help Desk or Cyber Security UK for guidance
- i. From the ScottishPower Cyber-Infrastructure never access on-line radio, audio and video streaming, instant messaging and webmail (such as Hotmail or Yahoo) and social networking sites (such as Facebook, Instagram, Twitter, Snap Chat, YouTube) unless specifically required and formally approved in advance for your job function.

The list above is not exhaustive and engaging in such activities when using the Company Internet may result in disciplinary action, which could result in the termination of your employment. For the avoidance of any doubt, the Company shall be the sole determiner of what constitutes prohibited, misuse and excessive use of the Internet.

3.5.3. Social Engineering

Social Engineering is where a person attempts to manipulate an individual to gain unauthorised information which can be used to damage the person or organisation either for criminal or competitive purposes. Therefore, Social Engineering attempts to exploit weaknesses in people, rather than systems or processes. Increasingly more sophisticated social engineering techniques are being used to appear more credible, particularly in email attacks.

Social Engineering phone calls may target staff in customer facing roles or customers and an attacker will try to convince the person that they have made contact with, that they are in a formal position of authority, or represent someone who is, and use this to obtain sensitive information. Such calls are often very convincing, as callers are highly skilled, confident and manipulative. You should remain vigilant and report any suspicious calls or requests for information to your line manager and Cyber Security UK.

3.5.4. Social Networking

There are many ways of distributing information on the Internet. When using Social Networking, you should be conscious that:

- a. As these Social Networking facilities will commonly contain information on an individual's actions, there may be a tendency to post information related to working life and employers such as ScottishPower. Comments posted on these Internet communication mediums may result in legal action against the Company, or other commercial damage and should be avoided
- b. When using Social Networking for business use, such as for information distribution purposes, you should be aware that such use is only permitted if it is in the course of employment and is authorised by the Company. You must take extra care, as you are expressly forbidden from:
 - i. Using your Company email address
 - ii. Making any public comments regarding the Company
 - iii. Making any negative or defamatory comments regarding Company suppliers, customers or colleagues
 - iv. Making comments about sensitive business-related or confidential topics, for example Company performance
 - v. Posting anything that Company suppliers, customers or colleagues could find offensive or inappropriate, including discriminatory comments, insults or obscenity
 - vi. Intimidating, discriminating, harassing or bullying colleagues
 - vii. Breaching company policies, legislation or ethical standards, for example give false or misleading information or making misleading statements.
- c. Company resources should only be used for legitimate business purposes when accessing or maintaining Social Networking sites. However, you should be aware that such Internet usage is closely monitored and subject to being screened by IT UK Security and reviewed by Cyber Security UK.

Please be aware that engaging in Social Networking activities and misuse of Company resources in particular unprofessional, inappropriate language and/or content which might be detrimental to the Company's reputation and business are not acceptable and may result in disciplinary action, which could result in the termination of your employment.



For the avoidance of any doubt, the Company shall be the sole determiner of what constitutes misuse, unprofessional, inappropriate language and content of social media activities.

3.5.5. Private Use of Social Networking

If you are a regular user of the Internet outside of work, this should be no concern of the Company. However, you should keep the following in mind to ensure that your use of the Internet is not detrimental to the Company:

- a. In your private use of the Internet, you should not express opinions about ScottishPower which may bring the Company into disrepute
- b. When using Social Networking in your private capacity, do not use your Company email address when communicating. You should avoid referring to your employment with the Company, unless that is the purpose of the specific Social Network, for example LinkedIn
- c. You should be careful not to bring the Company into disrepute when posting on social media or uploading information to the Internet, for example by uploading videos and photographs
- d. You should be careful to avoid social media communications which might be misconstrued in a way that could damage the Company's reputation, even indirectly
- e. If discussing or referring to the Company when using social network sites, you should make it clear that you are speaking on your own behalf, write in the first person and you must state that your views do not represent those of the Company
- f. You should remember that you have a responsibility for anything that you communicate and publish which will be available to a wide on-line audience
- g. If you are uncertain or concerned about the appropriateness of any statement or posting, you should refrain from making any statement until you have discussed it with your line manager
- h. If you see content on social network sites that are detrimental or reflect poorly on the Company or stakeholders, you should immediately contact your line manager and Cyber Security UK
- i. You must not do anything to jeopardise valuable Company trade secrets, other confidential information and intellectual property
- j. You must avoid misappropriating or infringing the intellectual property of other Companies and individuals, which may create liability for the Company as well as for you
- k. You must not use the Company's logo, brand names, slogans, trademarks or post any confidential or proprietary information without prior consent. Initially refer this to Group Internal Communications
- l. You must not use your business contacts made during the course of your employment. You will be required to delete or return all such details from your personal social network accounts on termination of your employment.

Please be aware that engaging in Social Networking activities, even in your private capacity, in ways that contravene the above guidelines or are otherwise unprofessional, contains inappropriate language and/or content which might be detrimental to the Company are not acceptable and may result in disciplinary action, which could result in the termination of your employment.

3.6. Virus, Encryption and Malicious Communications

ScottishPower Cyber-Infrastructure is under constant threat of attack from external parties who wish to access the Company's propriety information, obtain Personal Data for fraudulent purposes or merely to cause disruption to the Company's business. In addition, Company information is also at risk through hardware failures, power failures, system crashes or other problems. Business continuity plans and escalation procedures are used to ensure managed recovery from an incident arising from software or hardware failure.

Further information on business continuity is detailed on the Company Portal, Security section, Business Continuity Policy and the Group Security Policy.

3.6.1. Computer Virus

The term "virus" in relation to computer systems is used as a generic term to refer to all types of malicious software, including but not limited to spyware, key loggers, network worms, Trojan horses and logic bombs. In order to protect information and software on ScottishPower IT Systems, controls are required to prevent and detect the introduction of such malicious software.

- a. ScottishPower will mitigate against the loss or damage to the Company through computer viruses by ensuring:



- i. There are restrictions on the loading of unauthorised software on any ScottishPower IT System
 - ii. All Company PCs, servers and email gateways shall have up-to-date virus detection software loaded and activated
 - iii. All email will be scanned for malicious code as it enters and exits the ScottishPower network
 - iv. Users are responsible for ensuring that all Storage Media is scanned before use
 - v. Material downloaded from the Internet shall be for business use only. A check should be made before downloading to verify the material is sourced from a trusted site
 - vi. The playing of games and use of other personal entertainment on computer resources is strictly prohibited.
- b. Computer virus attacks can be difficult and expensive to identify and remove the source of infection. Please heed the following guidelines:
- i. You should be careful when viewing unsolicited emails or emails from untrusted sources. If you receive emails that fall into these categories, you should delete them unopened, which will reduce the risk of the virus being exposed onto Company systems
 - ii. Even emails from trusted sources should be treated with extra caution when opening attachments as email addresses are easily spoofed (hijacked)
 - iii. If you suspect that your computer has a virus infection, or experiencing unusual activity or a cyber-attack, you should immediately contact the Service Desk to log a fault.

All virus occurrences should be logged with the Service Desk and treated as security incidents.

3.6.2. Encryption

You should carefully consider the nature of the data being sent and what is the most appropriate method of communication. If a message is confidential, you must ensure that the recipient is comfortable with this means of communication. You should be aware that other persons may have access to the recipient's messages. If the content is highly confidential, other more secure means of communication should be considered. The Cryptography Rule and Cyber Asset Classification should be referred to in regards to encryption of classified material. You should be aware that:

- a. Internal emails are suitably protected and do not normally require encryption
- b. Encryption should be used where Protected Information/ Data is being transmitted externally. Users should raise a Service Request for email encryption using option "070 – Access Rights & Security" then "040 - Digital certificate for email encryption"
- c. You should only send encrypted emails where absolutely necessary
- d. Encrypted emails should not be sent as a default, as this will limit who can access your Encryption Certificate
- e. Laptop encryption is required by law not only to protect the information of the Company and any Customers stored thereon, but also to meet the security requirements of the GDPR. Laptops have encryption software automatically installed and you will be given the encryption password used. You must not try to bypass this encryption mechanism
- f. Any loss of Personal Data could result in significant fines for the Company. You therefore must take all reasonable measure to protect this information and immediately report any loss or theft through the agreed processes.

Failure to comply with the rules and requirements above and those highlighted in section 5.3 may result in action under the Company's Disciplinary procedure.

3.6.3. SPAM and Phishing

SPAM is unsolicited junk messages (email, telephone calls, instant messaging, SMS and more) sent indiscriminately in bulk, often for commercial purposes. Much of it is sent by botnets, networks of virus-infected computers, complicating the process of tracking down the spammers.

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and indirectly money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. Phishing attempts by telephone calls, SMS and instant messaging are now commonplace; if you believe that you are being targeted, avoid giving any personal or business information and terminate the communications courteously, but firmly. Ask for them to write to you, they should have the address, again not giving away any information.



IT UK Security and Cyber Security UK closely monitor SPAM and Phishing emails. SPAM filters are reviewed and updated regularly. If you receive an unsolicited or suspicious email, you should press the PhishMe button on the Outlook toolbar. This will report the email to and allow ScottishPower to take appropriate actions to analyse and prevent this becoming a larger problem. If, however you receive a phishing email after going to a website or otherwise providing your contact details online, you should reset your password for that site immediately and heed the advice given in this document.

3.7. Monitoring

ScottishPower routinely monitors Electronic Communications for all Users in line with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

ScottishPower reserves the right to withdraw any Electronic Communication facilities provided, if it considers that use of such facilities is in any way unacceptable.

3.7.1. Privacy of Electronic Communication and Physical Storage

- a. The Company operates its Cyber-Infrastructure for business related purposes, although it is accepted that you may occasionally use these resources in relation to personal matters. Further information on using Company resources for personal reasons may be found in the section “Limited and Reasonable Personal Use”
- b. The Company respects your right to privacy. The accessing of the contents of personal electronic communications will be avoided wherever possible; however, the Company does reserve the right to access personal electronic communications as part of its monitoring or investigation processes
- c. CCTV images are recorded and monitored for purposes of Crime Prevention, Detection, Site Safety & Security.
- d. You should be aware that your usage of the Company’s Cyber-Infrastructure, services and the Internet is logged, monitored and audited. By accessing the Company’s systems, you are deemed to have consented to the monitoring of, but not limited to:
 - All emails - sent or received
 - Mail boxes and private directories
 - All use of the Internet and all other communications techniques deployed when you use Company systems and resources
 - All files held on ScottishPower IT systems
 - All telephony conversations, unless made from call boxes or personal mobile phones.
- d. Items marked “Personal” such as paper documents, electronic files or folders and email messages (including those marked as “Personal” in the subject header) are not afforded any greater level of privacy than other items. You should be aware that any data that is collected stored or transmitted on the Cyber-Infrastructure may be subject to monitoring. Should you wish to make an Electronic Communication that is strictly private or personal in nature, this should not be made using Company resources
- e. Use of the Company telephony systems also constitutes providing consent to monitoring of communications. As such you should be aware that calls made using Company telephony equipment are not deemed private. Should you wish to make a private telephone call, you should use your personal mobile telephone or other means of communication
- f. Use of physical storage space constitutes providing consent to monitoring of storage spaces e.g. lockers, desk drawers and cupboards
- g. The Company’s monitoring practices and procedures have been developed with full consideration of the GDPR and the Information Management Rule and the Information Commissioner’s Employment Practices Code.

3.7.2. Monitoring Methods

- a. In line with the Information Commissioner’s Code of Practice (The Employment Practices Code - Part 3: Monitoring at Work), the Company has undertaken an impact assessment of its current monitoring methods to:
 - Examine the Company’s legal obligations



- Identify the benefits of monitoring
 - Identify any potential adverse impact on Users
 - Consider any alternatives to monitoring.
- b. As an outcome from this assessment, the Company has confirmed that the monitoring arrangements in place are proportionate to the legitimate business needs of ScottishPower which includes, but is not limited to:
- Use of Company Cyber-Infrastructure devices
 - Internet communications and usage
 - On an on-going basis, the Cyber-Infrastructure may be scanned to identify suspicious files or activities
 - On occasion the Company may deem it necessary to monitor telephone calls made using ScottishPower equipment in connection with a security investigation.
- c. Monitoring of communications conducted using Company resources will:
- Encourage responsible and efficient use of the Company's electronic communication resources
 - Maintain the confidentiality, integrity and availability of the Company's IT infrastructure and information services
 - Guard against damage to the ScottishPower brand and reputation
 - Help to ensure compliance with all applicable laws and regulations, including Data Protection, Copyright and Licensing Laws.

3.7.3. Investigations

- a. Suspected misuse of the Company's Cyber-Infrastructure may be detected as a result of the monitoring methods ScottishPower has in place, or as the result of a complaint received from an internal or external party
- b. No investigation, either preliminary or full, will be undertaken without prior engagement with HR via 1HR Direct and/ or Legal
- c. Once authorised to investigate, Cyber Security UK will undertake an investigation into the suspected misuse
- d. No person shall monitor, assess or investigate a suspicion or detection of IT misuse, whether preliminary or full. All IT investigations will be conducted by Cyber Security UK.

4. Roles & Responsibilities

This section provides general expectations on the allocation of roles and responsibilities in the organisation and should be supplemented where necessary with more detailed expectations within each ScottishPower business area.

4.1. All Users

All Users with access to or using ScottishPower Cyber-Infrastructure must be aware of their rights and responsibilities and must comply with the Rules, Policies, Guidelines and procedures of the Company. Specifically, all Users must:

- Undertake all mandatory training courses
- Ensure that their handling of Company Protected Information/ Data is in line with the provisions of the relevant Rules
- Notify the Data Privacy Manager (DPM) and the Data Privacy and Protection (DP&P) team of any data loss
- Notify your manager and Cyber Security UK of any suspected or known breach of this Rule.

4.2. Managers

Business/department managers shall promote:

- The day-to-day implementation and compliance to the Policy



- Ensuring that users are made aware of ScottishPower policies, rules and procedures
- Following user recruitment and termination processes, ensuring that access is promptly removed when a user leaves employment \ engagement with ScottishPower
- Taking appropriate action when a breach or non-conformance with the Rule is suspected or confirmed, and communicating with Human Resources.
- Deactivation and removal of access on termination or employment
- Deactivation and removal of access that is no longer required on job move or changing in role.
- Responsible for retrieval of all ScottishPower equipment on leaving the company.

4.3. Human Resources

Human Resources shall be responsible for providing advice and guidance on the Policy to employees and for providing advice to managers on appropriate actions resulting from breaches of the Policy.

4.4. Cyber Security

Cyber Security shall be responsible for:

- Governance, oversight and approval of the Policy including the maintenance and documentation of the controls associated with the Policy.
- Monitoring and measurement of the level of adherence to the Policy.
- Providing advice, guidance and clarification for users on the contents of the Policy.
- Rule awareness & training.

4.5. Corporate Functions and Business Areas

Corporate Function and Business Areas shall be responsible for:

- Identifying the required technical tools and technologies needed to meet the defined controls.
- Provisioning and implementing the necessary technical controls (as defined) to support the Rule.
- Technical security monitoring and measurement of technical tool sets to ensure that technical controls are working as expected.

4.6. Reporting

If you suspect a Security Breach or misuse of the ScottishPower Cyber-Infrastructure by another individual, you must report this to their line manager. The line manager should contact 1HR Direct who can advise whether a formal investigation is required under the Company's Disciplinary Policy and Procedures. Under no circumstances should you conduct an investigation independently or prior to contacting 1HR Direct.

Further information is detailed in the Reporting and Whistle-blower Policy which can be found on the Company Portal.

5. Compliance

5.1. Compliance Measurements

ScottishPower must comply with all relevant legislation, regulations and Court Orders as they relate to various security matters. In addition to defining corporate responsibilities, there are several pieces of legislation that define personal responsibilities for Users. All Users must be aware of relevant legislation and compliance requirements as it relates to their job function. In particular those individuals with accountability for maintaining corporate compliance with such legislation are duty bound to ensure full understanding of legislative requirements and robust compliance across the business.

In order to maintain compliance with relevant legislation and regulations, ScottishPower will conduct regular compliance monitoring which may take the form of reviews, audits and internal assessments. Internal or external auditors may carry out such compliance monitoring checks. In addition, Cyber Security UK and Internal Audit have the appropriate skills and experience to carry out informal reviews and provide advice and consultancy on legislative and regulatory compliance issues as they relate to Security.



5.2. Compliance Mapping

- Civic Government (Scotland) Act 1982
- Companies Act 2006
- Computer Misuse Act 1990
- Copyright, Designs & Patents Act 1988
- Data Protection Act 2018
- Defamation Act 1996
- Employment Practices Data Protection Code
- General Data Protection Regulation 2018
- Iberdrola's Code of Ethics
- Police and Criminal Evidence Act 1984
- Privacy and electronic Communication (EU Directive) Regulations 2003
- Telecommunication (Lawful Business Practice, Interception of Communications) Regulations 2000

5.3. Related Company Rules and Policies

This Policy relates to the following Rules and you can find the full content for each at the following locations:

- Access Governance Rule
- Clear Desk Policy
- Cryptography Rule
- Data Extract and Handling Rule
- Data Protection Policy (ScottishPower)
- Exception Management Rule
- Exception Request and Risk Acceptance Agreement
- HR Security Rule
- Information Management Rule
- Information Protection User Guide
- Mobile Phone Policy
- Mobility Rule
- Personal Data Protection Policy (Iberdrola).
- Risk Assessment and Exception Management Rule
- System Acquisition, Development and Maintenance Rule.

Further Policy information as referenced in this document is detailed on the Company Portal:

- Business Continuity Policy
- Code of Ethics
- Group Security Policy
- Guidelines for Personal Account Management
- Reporting and Whistleblower Policy.

5.4. Non-Compliance

Users in breach of and/or not conforming to the Policy shall be considered to be in breach of the Policy which may result in action being taken under the Company's Disciplinary procedure.

Individuals hired through a temporary employment agency, a contractor or a consultant in breach of and/or not conforming to the Policy can result in the termination of their assignment / placement with the Company.



5.5. Guidance and Useful Contacts

To raise an IT related incident, either log in to the Service Request system using the link on the Company Intranet portal, on your workstation Start menu go to “My Corporate Applications” then “IT Requests and Incidents” or call one of the numbers as listed below:

- 131 or 02392 638023 for Retail
- 132 or 02392 638021 for Networks
- 133 or 02392 638020 for GEM / Renewables
- 137 or 02392 638018 for Corporate

