ICT and Data Security Policy

Approved: Apr 21
Next Review: 2024

ROSEHILL HOUSING CO-OPERATIVE LIMITED
250 Peat Road, Glasgow G53 6SA
Tel: 0141 881 0595
Email: admin@rosehillhousing.co.uk
Website: www.rosehillhousing.co.uk

1. Introduction

1.1 Internet, Electronic communications (both internal and external) and other ICT systems are vital for Rosehill Housing Co-operative's (Rosehill) business processes. However, they also can expose us to serious risks. These risks include loss of data, unauthorised access to our systems and data, retaining data for longer than is necessary, and careless use of email, social media and the Internet and so on. For example, confidential information may be deliberately or accidentally sent to the wrong people. In addition, misuse of the Internet and emails can introduce viruses/malware into our network, infringe copyright laws and result in the harassment or defamation of others.

1.2 Posting personal opinions on social media sites can have serious implications for both Rosehill and the individual(s) concerned. For these reasons, and others, we have to impose tight security systems and rules about access to our systems, data storage and security, and certain limitations on Internet, email and social media use in relation to both business and personal use. We also have to set rules in place for how our ICT equipment is accessed and used and how our data is stored.

1.3 This policy covers all our employees, management committee members, and third parties with access to our systems with our permission.

2. Definition of ICT and Data Security

2.1 ICT and data security refers to measures, controls and procedures applied by us, or on our behalf, in order to ensure integrity, security, confidentiality, availability and protection of our ICT systems and data.

3. Our Approach

3.1 This document sets out the rules for how we keep our ICT systems and data safe and secure. It also details the approaches we take to keep data safe and secure. It applies to everyone who uses our ICT systems, whether they are used at our offices or remotely.

3.2 This Policy also refers to how our systems and devices may be used. However, we have a separate Policy, ICT - Acceptable Use Policy which provides greater detail on this.

3.3 The purposes of this policy are to:

- ensure that all ICT systems and other communication equipment and resources are used correctly and kept secure, including password complexity requirements
- establish our approach to data and information security
- set out how we control access to our data and information

- establish clear rules on how email, Internet, social media and telephone facilities (both in the office and remotely) should be used, including personal use and advises that automatic monitoring, of email and internet use takes place and the reasons for it

- provide clear guidance on the disposal of ICT equipment and the secure destruction of data

- provide clear guidance on the importance of change control when managing system configuration changes, implementations and important documentation

3.4 Any breach of this policy will be taken seriously and may lead to disciplinary action. In serious cases this could include summary dismissal under our disciplinary procedure. If the effect or meaning of any part of this policy is unclear guidance should be sought from the Director.

4. Other Relevant Policies

4.1 This Policy is linked and should be read in conjunction with the following policies:

ICT – Acceptable Use Policy
Privacy Policy

5. ICT System Use

5.1 Hardware Provisions and Security

5.1.1 Desktop PCs, thin clients, laptops, tablet computers, desk telephones, mobile phones, and shared office equipment such as printers, photocopiers and document scanning facilities have been provided to ensure we are well equipped to serve our tenants and other customers, facilitate office functions, allow access to office software applications, support mobile working arrangements and printing and so on.

5.1.2 Security of equipment is the responsibility of the staff member(s) to whom it is allocated and it must not be used by anyone else, other than in accordance with this policy. General equipment, such as photocopiers or printers located in communal areas is the joint responsibility of all staff members within the organization.

5.1.3 The Finance Manager will hold records, by asset tag, and serial number of all equipment currently in use and also the staff member or section these have been allocated to.

5.2 Network and Software Application Security

5.2.1 Our network is secured by passwords and various software packages and

can only be accessed by devices configured by our IT support provider Omniledger. Software applications in use within Rosehill are mainly stored centrally on servers accessed by individual PCs, thin clients, laptops and tablets, or can be hosted and accessed via the Internet or loaded on to individual devices including mobile phones. All of these require some form of identification, such as a network user logon, an application specific user logon or, for a mobile device, a unique username/password combination or a passcode to gain access. These should comply with the password policy, within this document.

5.2.2 Security of user logons and passwords for individual user areas and access to software applications are the responsibility of each individual staff member and they must not be used by or divulged to anyone else, including our support provider Omniledger, under any circumstances

5.2.3 We test our network and software annually, for vulnerability to hackers, and take action to remedy any issues found.

5.3 Operating Systems & Devices

5.3.1 Only current operating systems may be used to access our network and systems. Currently, this means nothing older than Windows 8.1, under extended support by Microsoft until 10th January 2023. Steps will be taken to upgrade operating systems, in conjunction with Omniledger, our IT support provider in advance of extended support arrangements ending.

5.4 Web Portals & Cloud Based Storage

5.4.1 We do not yet provide web portals.

5.4.2 Cloud storage is provided as part of our disaster recovery planning. Data is transferred to a secure data centre in Stevenage, Hertfordshire. This data is core to the recovery of Rosehill servers in the event of a loss of servers at head office, This service is managed and maintained by OmniLedger and checked on a daily basis. All data is transferred using secure encrypted data transfer protocols. Data is retained in the data centre on a 7 day rolling cycle.

5.5 Viruses, Malware & Phishing

5.5.1 The introduction of a virus or malware into our ICT systems could be devastating. These are malicious/unwanted computer programs designed to compromise security or data/information. Our IT support provider is responsible for ensuring that suitable security mechanisms and security software is installed, but this does not necessarily guard against all viruses or malware, as new variants are developed on a daily basis. (Mobile phones should be protected by ant-virus software as advised by Omniledger and installed locally by users.) Users should be aware that viruses and malware can be introduced via email attachments, CD-ROMs, memory sticks etc. and the Internet.

5.5.2 Phishing is the attempt to acquire sensitive information such as usernames, passwords or credit card/bank details (and often the finances or information these protect) by masquerading as a trustworthy entity in an electronic communication.

5.5.3 “Fake” communications that pretend to be from colleagues, banks, social web sites, auction web sites or even ICT administrators are commonly used to “trick” unsuspecting users into accessing them. Phishing emails may contain links to websites that are infected with malware or are fake copies of legitimate web sites. These entice users into entering secure and confidential details such as usernames/passwords or bank details, which are then used to compromise security or finances. Money must never be transferred to an outside account on the strength of an email or telephone call; staff must verify all information by calling the organisation involved using their publicly available phone number. If in doubt, do not do anything without checking and checking again.

5.5.3 Links to web sites or other information that are contained within emails or distributed via social media sites should always be treated as suspicious, unless you are absolutely certain that the link is from a trustworthy source and you are expecting it or can verify it prior to accessing the link. As highlighted above, many phishing attacks and malware are initially spread or accessed by users clicking on links within emails or that appear on social media sites.

5.5.4 It is the responsibility of each user, to take care when opening email attachments, especially when they are not expected or they are from unknown sources. If there is any doubt about an attachment or the sender, you should contact our IT support provider Omniledger, who will check whether it is safe to open the attachment. Suspicious emails should not be forwarded to anyone else as this could make matters worse, by spreading the potential threat.

5.5.5 Staff members should not install or attempt to install any software onto PCs, laptops or tablets that has not been approved or purchased and licensed by the company, nor download any software applications or material (including games and screen savers) from the Internet, CDs, DVDs or memory sticks etc. without first obtaining the approval of Omniledger, and then only for business purposes. To ensure this does not happen indiscriminately, users have limited access rights which restrict their ability to install, remove or share data from our system. Mobile devices such as phones and tablets can access Apps from the official Google Play app store, but staff must not download anything without prior approval from the Director. Google Play Protect helps keep devices safe and secure:

- It runs a safety check on apps from the Google Play Store before they are downloaded.
- It checks devices for potentially harmful apps from other sources. These harmful apps are sometimes called malware
- It warns about any detected potentially harmful apps found, and removes known harmful apps from devices or it may by prompt the user to do so.

5.5.6 The ability to connect devices, adapters, equipment or install media which has not been provided by Rosehill to our ICT systems, without prior approval of Omniledger, has been restricted to protect our systems. This includes items such as MP3 players, mobile phones, memory sticks, CDs and DVDs or other devices/accessories that connect via USB ports. USB ports on office PCs have been disabled but this will be kept under review.

5.5.7 Access to certain types of web sites is controlled through a web filter (Open DNS) which categorises sites (e.g. Drugs, Pornography, and News etc.). The web filter has been configured to actively block certain categories of websites that are deemed inappropriate for business use (such as Pornography) and they will instead display a “site blocked” warning message and be inaccessible to users. It is possible that the web filter might sometimes incorrectly categorise certain web sites. It is also possible that new web sites may not be categorised and therefore be wrongly deemed inappropriate. There may be cases where access to web sites is restricted in error. All instances of this nature should be reported to Omniledger who are responsible for configuring the web filter rules. Sites you need for work purposes can be unblocked by calling Omniledger. (Refer to our ICT Acceptable Use Policy for further guidance on usage)

5.5.8 Rosehill currently use Symantec Endpoint Security Enterprise Edition and Symantec Cloud.Protect to provide Anti-Virus protection. Licences for Symantec products are supplied by OmniLedger and maintained and checked daily as part of the on-going enhanced support services.

5.6 Cyber Crime & Computer Misuse Act (1990)

5.6.1 The Computer Misuse Act of 1990 is a law in the UK that makes illegal certain activities, such as hacking into other people’s systems, misusing software, helping a person to gain access to protected files of someone else's computer or introducing malware into computer systems (viruses, trojans, spyware etc.). This is cyber-crime.

5.6.2 The Act itself was created in 1990 and it is safe to say that computer technology and especially the Internet has changed dramatically since its introduction. Social Media is just one primary example. However the principles contained within the Act can be fully applied to the Internet of today and are still completely relevant.

5.6.3 The Act recognises the following offences and penalties:

5.6.3.1 Unauthorised access to computer material (Part 1)

This is the lowest level of offence and is one that many of us might be guilty of at some stage in our working lives. If you find, guess or use someone else’s’ password to log onto their user area, even if you do this to look at their files, even if you don't change, delete or damage anything, you are still guilty of accessing materials without authorisation - and this is illegal. This offence carries the risk of being sentenced to six months in prison and/or a hefty fine. This does not affect authorised access for a legitimate business reason but

this must only be done by a senior manager e.g. in times of long-term absence.

5.6.3.2 Unauthorised access with intent to commit or facilitate a crime (Part 2)

The difference between this and the first offence is that the person gaining access to someone else's' system has done so with the sole purpose of doing something illegal. This might mean that they had to guess or steal the password in order to get into someone's user area or their bank account. They could do this by trial and error or by using special programs such as spyware or key-logging software, or they could use a technique called 'phishing'. They might want to steal company information/data or access secure bank details or funds. This offence carries the risk of up to a five year prison sentence and/or a hefty fine.

5.6.3.3 Unauthorised modification of computer material (Part 3)

Everyone deletes files from their own system, maybe they no longer need them or maybe they delete them by mistake. This is absolutely fine as there was no intent to cause any damage. This offence relates to the deletion or changes made to files with the intent to cause damage to an individual or company. The difference is 'the intent to cause damage'. This offence also covers purposely introducing viruses or malware to another individuals or companies system. If you knowingly transmit a virus or malware to others, you are guilty under this section of the Computer Misuse Act. This offence carries a penalty of up to five years in prison and/or a fine.

5.6.3.4 Making, supplying or obtaining anything which can be used in computer misuse offences (Part 3a)

Making — This includes the writing or creation of computer viruses, worms, trojans, malware, malicious scripts etc.

Supplying — This part covers the distribution of any of the above material whether you have created it yourself or obtained it from elsewhere. It is an offence to supply or distribute these files to others.

Obtaining — If you purposely obtain malicious files such as computer viruses or malicious scripts that you know could be used to damage computer systems then you have committed an offence under the Computer Misuse Act.

This offence carries the risk of up to a five year prison sentence and /or an unlimited fine.

5.7 Wireless Technology

5.7.1 Wireless technology (Wi-Fi) and wireless devices are now commonplace. Staff authorised to work remotely will normally connect to our servers via their home

network, however it is accepted that this might not always be the case. Wi-Fi networks can be unsecure (open) and secure (require a password to access). Secure networks also have different levels of security. When you are looking for an available Wi-Fi network, alongside the network name that appears (SSID) you should also see an indication of whether the network is secure or unsecure and also the level of security (encryption type) the network offers. These are the most common security levels available with guidance in whether to trust and connect to the network or not:

Security/Encryption Type	**Should I Connect To This Network?**
Open/Unsecure	No - do not connect
WEP	No - do not connect. No longer secure enough
WPA (TKIP)	WPA2 is better, but WPA is ok for a "short" time
WPA2 (AES)	The preferred Wi-Fi network security type
Other	No other network type should be used
Free/Public Wi-Fi networks, in coffee shops, libraries etc.	These should only be used for work purposes when there are no alternatives available

5.7.2 Even if a Wi-Fi network is secure and WPA2 (AES) encrypted, you should always check with the network provider that the network you wish to connect to is valid and that you have been given the correct password details, before any attempt is made to connect. Sometimes Wi-Fi networks can be "fake" and appear to have recognisable names of nearby shops etc. to lure unsuspected users into connecting to them (e.g. McDonalds, Starbucks etc.). Particular care should be taken when using these sorts of networks.

5.7.3 Mobile devices (laptops, mobile phones, tables) and other Wi-Fi capable devices should be configured such that they do not detect or connect to wireless networks automatically. This should be a manual process, by the user only, following security checks (recommended above) and confirmation that it is a valid and secure wireless network. It is the responsibility of the staff member using the device to ensure these settings remain disabled. (Disabling the Wi-Fi capabilities of a device can also extend battery life.)

5.7.4 Bluetooth connectivity on mobile devices should be disabled by default and only enabled if connection is necessary to a known external device. It should not be used to pair any unauthorised external devices, as this could lead to the mobile device being compromised.

5.7.5 Rosehill's wireless network is secure and access is controlled by the Director who must authorise access. We have a guest wifi network which is available to users of our Committee Room and to others when providing services to us e.g. provision of training. The guest wifi is also used by Committee Members for meetings. Authorised access is also available to consultants and other persons who need to access our systems when providing services to us, such

as audit. The Director, or someone acting under her authority, will set up access and input any passwords which will always be kept secret from external people.

5.8 Remote Working, Travelling, using USB Memory Sticks and Similar

5.8.1 The Director can authorise staff to work remotely, usually from home. At this time remote working is limited to home working only. Access to our systems will be via devices supplied by us via an L2TP Virtual Private Network connection, which is encrypted with a username/password combination and, for more advanced security, also a passphrase that is only known to our support providers.

5.8.2 This enables staff to work remotely on their own desktop and on files which do not leave our servers thus protecting data security. Paper files which contain personal/sensitive data must never be removed from the office, even for home working. If staff need to access paper files they should be scanned on to our system and accessed remotely.

5.8.3 Given the amount of confidential information, which is accessible remotely, sensible precautions must be taken when devices such as mobile phones, tablets and laptops are taken out of the office for this purpose. In particular, ICT equipment must not be left on view inside a vehicle, whether inside a bag or not. If you have to leave such an item unattended in a vehicle, it must be locked away in the boot or glove compartment. If you are travelling on public transport or are in a public place, keep your equipment with you at all times or, if this is not possible, in sight. Users will be provided with appropriate means of carrying equipment such as laptop bags or cases.

5.8.4 Financial, sensitive or personal data must not be stored locally on any devices used for remote working; all such data must only be accessed by a device connecting to our servers or to a cloud service set up by us for that purpose. If an unencrypted device was lost or misplaced and, as a consequence, this type of data was released into the public domain it would breach the UK General Data Protection Regulation (GDPR). Financial, sensitive or personal data must also not be stored on any USB memory sticks, memory cards or any other portable storage media including CD and DVD. These sorts of items are too easily lost.

5.8.5 If you are working in a public place, you must position yourself so that other people cannot read documents that you are working on and/or see passwords you are typing in. This applies whilst working at home too.

5.8.6 When using mobile phones, do not discuss private matters relating to company business or that of our tenants, other customers and partners if you think you may be overheard by anyone who is not a work colleague. (Particular care must be exercised in and around our reception area.)

5.8.7 Users are reminded that it is an offence to use a mobile device when driving. Staff members should therefore not use mobile devices, with or without a hands-free kit, for any purpose when driving on Rosehill's business, this includes driving from one place to another e.g. to a training course from the office.

5.8.8 It is therefore recommended that mobile devices are switched off or set to silent when driving to avoid distractions.

5.9 Computer/Device Access Control & Password Guidelines

5.9.1 Introduction/Purpose

5.9.1.1 The purpose of these guidelines is to make sure all our resources and data are covered by adequate password protection. The guidelines apply to all employees who are responsible for one or more account or have access to any resource that requires a password, including accounts held by others including banks, suppliers and so on. (When logging in to accounts held by others you should follow their guidance on password length and complexity and this policy where there is no guidance but subject to their system limitations)

5.9.1.2 These guidelines assist staff to create computer passwords, in formats which are sufficiently strong, and gives advice on keeping passwords secure.

5.9.1.3 Staff access a variety of IT resources, including computers, photo-copiers and other hardware devices, our network, data storage systems, and other accounts and software. Passwords are a key part of our strategy to make sure only authorised people can access those resources and data.

5.9.1.4 All employees who have access to any resources, which require a password, are responsible for choosing strong passwords and protecting their log-in information from other people.

5.9.2 Password Creation

5.9.2.1 When it is necessary to create new users e.g. when a new member of staff joins, this will be done by Omniledger under authorisation by The Director; initial passwords will be temporary and set by Omniledger to expire immediately and users will be prompted to replace the temporary password on initial sign on and thereafter they will be set to expire every six weeks at which point they will need to be changed. Where access is created to resources locally, e.g. to the photocopier this will be done by the Customer Services Officer but with all password inputs by the member of staff.

5.9.2.2 All passwords should be reasonably complex and difficult for unauthorised people to guess. Staff should choose passwords that are at least eight characters long and contain a combination of upper and lower-case letters, numbers, punctuation marks and other special characters. These requirements will be enforced with software when possible, but are subject to systems limitations and, in these circumstances password complexity rules should be followed as far as possible. Some of our systems, such as Omniledger, will block users after a certain number of failed password attempts. Users must email Omniledger requesting to be unblocked and then follow any instructions received.

5.9.2.3 In addition to meeting the above requirements, staff must also use common sense when choosing passwords. Basic combinations that are easy to crack must be avoided. For instance, choices like “password,” “password1” and “Pa$$w0rd” are equally bad from a security perspective. Also, avoid using names of memorable places such as, for example, a holiday destination, as these are very likely to be known to other staff. Also, it is not acceptable to update a password simply be changing a number at the end e.g. Edinburgh326 to Edinburgh880 and similar.

5.9.2.4 A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase “This may be one way to remember” can become “TmB1WTr!”

5.9.2.5 Staff must choose individual unique passwords for all of their company accounts, and may not use a password that they are already using for a personal account. All passwords must be changed at least every 6 weeks This requirement will be enforced using software when possible. If the security of a password is in doubt, for example, if it appears that an unauthorised person has logged into an account or other resource, the password must be changed immediately. If the security of a password is in doubt, for example, if it appears that an unauthorised person has logged into an account or other resource, the password must be changed immediately.

5.9.3 Mobile devices

5.9.3.1 Mobile phones, tablets and laptops must be protected by a password or PIN configured so as to be required at power on and screens set to auto-lock when idle for a short period of time. Devices must not be used until these protections have been activated either by the user or by Omniledger. Staff must not alter these settings or attempt to disable them.

5.9.4 Protecting Passwords

5.9.4.1 Staff must:

- Never share their passwords with anyone else in the company, including colleagues, managers, administrative assistants, IT support companies/advisors etc. Everyone who needs access to a system will have their own unique password

- Never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system. If using remote assistance, it is permissible for you to input your password, without disclosing it, at the direction of our IT support company

- Take steps to avoid phishing scams, as set out previously, and other attempts by hackers to steal passwords and other sensitive information.

- Must refrain from writing passwords down and keeping them at their workstations. (See above for advice on creating memorable but secure passwords)

- Must not use password managers or other tools to help store and remember passwords unless these have been provided by us as part of our systems

For the avoidance of doubt, on termination of your employment for whatever reason, you must provide details of all your passwords, to your line manager, so that ICT system and device security can be updated, controlled and maintained.

5.10 Email Security

5.10.1 It is very easy to send an email to the wrong person. You should be very careful to ensure that the emails you send are correctly addressed, particularly when they contain information that you would not want others to see. To assist with this, email recipients should be chosen by selecting the "To" button and clicking on the name in the address book displayed where possible.

5.10.2 Remember that email is not a secure way of sending information. Emails can be intercepted by third parties and intended recipients can alter and/or forward emails without your knowledge. You should therefore never include any personal, sensitive information in the body of an email. All such information should be sent as an attachment and the attachment should be protected by a password and headlined as private and confidential. This applies to both internal and external emails, and the password should be notified to any external recipients by text preferably or by phoning but if absolutely necessary by a separate email. It is important that copies of sent documents saved to our systems are not password protected to ensure they can be accessed in future.

5.10.3 For internal emails, if you are sending personal, sensitive information which is held in a shared folder which the recipient(s) has access to, then you should insert a hyperlink to the document within your email instead.

5.10.4 Deletion from the inbox or archive, or any email folder does not mean that

emails are instantly deleted, this is done when the recycle bin is emptied.

5.10.5 Email access is via a user's unique network logon, which is password protected or via a user's mobile device, which is protected by a PIN, finger print or passphrase etc. Unauthorised access to email using another member of staff's logon will result in disciplinary action unless such action has been authorised by the Director, in specific circumstances such as long term absence.

5.11 Cyber Security

5.11.1 With the increased use of digital technology and the use of computers, smart devices and internet being part of our everyday lives, cyber security is more important than ever. Therefore, it is crucial that we have measures in place to reduce the risk of Rosehill becoming a victim of cyber attack.

5.11.2 As well as the measures set out in this Policy we have further improved our Cyber Security by attaining Cyber Essentials Certification. This is renewed on an annual basis. We want to assure our tenants, customers and stakeholders that we take the protection of our IT systems and data seriously. To this end we display the Cyber Essentials branding on our website.

6. Information Security

6.1 We hold personal and sensitive personal data and information on tenants, housing applicants, employees and so on. We make all reasonable attempts to store data in electronic format only, however some hard copy data requires to be retained and stored.

6.2 Where we store a physical copy of data we take the following measures to ensure that it is kept secure and only seen by those staff who need to see it:

- During the working day we ensure that no files are left where they could be seen by an unauthorised person
- We operate a "clear desk" policy, at the end of the working day no paperwork which contains personal information is left lying on desks
- Paperwork is put away in locked filing cabinets, cupboards or drawers
- Files which are archived are kept in a locked, windowless file room with access restricted to authorised staff

6.3 We store most of the data we hold in electronic format, we take the following measures to ensure that it is kept secure and only seen by those staff who need to see it:

- Information is held on central servers and not on individual PCs and laptops
- Access to our servers is protected by password with additional passwords to access information
- Access to personal information is restricted to authorised staff e.g. only certain staff get to see sensitive information such as rent arrears
- Information which is transmitted electronically is protected by password

7. Disposal of Equipment & Secure Destruction of Data

7.1 Disposal Of Equipment

7.1.2 When ICT equipment reaches the end of its useful life and is due for replacement, a number of options are available, to dispose of the equipment, in the following order:

- Consideration should be given to donating the equipment to a local charity or community project for reuse.

- The equipment can be sold to other outside organisations or given to Committee or staff members where there is no re-sale value.

- The equipment could be disposed of in an environmentally friendly manner using a specialist contractor to wipe all hard drives and provide a certificate confirming that all hard drives have been wiped. This task must be completed on our premises.

In all instances where equipment is being disposed of, express consent must be given by the Director, and all hard drives must be wiped.

7.2 Secure Data Destruction

7.2.1 The overriding consideration in the disposal of ICT equipment is to ensure that all of the data residing in or on the equipment is securely destroyed, to satisfy the requirements of the UK GDPR.

7.2.2 All hard disks that are to be reused or recycled should be securely wiped using a specialist “wipe” utility such as “DBAN”. These utilities make multiple passes over the disk, writing meaningless data, to ensure that all data has been overwritten and is completely inaccessible. A minimum of 3 passes is recommended.

7.2.3 All hard disks that are to be disposed of and not reused should be physically dismantled and destroyed, this should be done by a reputable company which provides appropriate certification. In the case of Server equipment, this should be arranged by Omniledger.

7.2.4 Other forms of media, such as CD, DVD,or USB flash drives and data tapes should never be sold or donated to any other organisation or individual, but always be physically destroyed.

7.2.5 Mobile phones or tablet computers, if they are to be recycled, should be first securely erased and reset to “factory defaults” using the correct built in utility (normally found within the settings section of the device).

8. Managing Configuration Changes, Updates and Upgrades

8.1 Change Control

8.1.1 In relation to PCs, thin clients, servers and our network, related ancillary equipment, and software and software packages, all changes will be implemented by Omniledger, or overseen by Omniledger or cleared with Omniledger prior to any other company being involved. Every configuration change that is requested by staff members that involves updates or amendments to ICT security within software applications, Microsoft networking, physical hardware devices or other access control mechanisms, must be approved via the following processes:

Change Requested	**Approval/Authorisation Required**
Changes to Active Directory Users or groups	Director
Changes in access to shared/public folders	Director
Add or remove users	Director
Add or remove remote users	Director
Changes to user access levels	Director

Change Requested	**Approval/Authorisation Required**
Changes to existing software, software modules or installation of additional modules	Director
Report writing	Section Head
Changes to any ICT hardware or security mechanism (e.g. Telephone System, Internet Firewall)	Director
Access to another users mailbox or send on behalf of permissions	Director
Access to blocked email file attachments	Not required
Other request/security change	Director

8.2 System Maintenance

8.2.1 Support arrangements are in place with Omniledger, covering all network resources and software. As part of their support service, they will be on site at least four times per annum to perform system checks, optimisations and updates. These visits will also be utilized to troubleshoot as necessary and for staff training where needed.

8.3 Hardware and Software Updates, Upgrades & Implementations

8.3.1 Every configuration change that is necessary due to an ICT software upgrade, hardware upgrade, system review or a new implementation must first be approved/authorised by the Director in consultation with Omniledger.

8.3.2 All Microsoft security patches and service packs must be approved and installed by Omniledger where these don't happen automatically.

8.3.3 All other security patches and service packs must be approved for installation by Omniledger.

8.3.4 All recoveries of files, software applications or Servers from backup storage must be authorised by the Director.

8.3.6 All software and hardware installations/implementation projects, including equipment upgrades or additional equipment, must first be approved by the Director and installed or configured by Omniledger.

8.3.7 All other network level configuration changes that are not specifically mentioned already should be notified to the Director.

9. Right to Access our systems

9.1 We may disable or restrict any staff member's access to any of our ICT Systems, including email and internet access, at any time. We will only do so with good reason, for example if you give, or have been given, notice of the termination of your contract.

10. Data Protection

10.1 On the 25th May 2018 the legislation governing data protection changed with the introduction of the General Data Protection Regulation (GDPR). Following the UK's exit from the EU, and the end of the transition period which followed, the GDPR formed part of the retained EU law and became the UK GDPR which together with the Data Protection Act 2018 constitute the UK's data protection legislation.

11. Equality and Diversity

11.1 We are committed to ensuring equal opportunities and fair treatment for all people in our work. In implementing this Policy, we will provide a fair and equal service to all people, irrespective of factors such as gender, race, disability age, sexual orientation, language or social origin, or other personal attributes.

12. Risk Management

12.1 In all key areas of our business we need to consider any risks which may arise. To this end we have in place a robust Risk Management Policy and from this

flows our Risk Register. We have identified our material risks which are regularly monitored by our Management Team and Audit Sub-Committee.

12.2 To ensure we continue to manage the associated risks we will periodically review this policy to ensure compliance with all legislative requirements and regulatory and best practice guidance.

13. Review

This policy will be reviewed at least every three years to ensure it continues to comply with all required legislation.

App May 18
Reviewed 2021
Next Review 2024