TAI CANOLBARTH CYMRU
MID-WALES HOUSING

Yn barod **amdani** **Equal** to the challenge

Gofal a Thrwsio ym Mhowys
Care & Repair in Powys

Mid-Wales Housing Group Electronic Communications & ICT Security Policy

Strategic Aim:	To ensure that all ICT systems, other communicating equipment and resources are used correctly and kept secure.
Reference No:	ICT Security Policy v1.1 January 2015
Date Of Issue:	30th January 2015
Next Review Date:	January 2018
Departments Affected:	All Departments
Approved By/Date:	Board Of Management 28th January 2015
Lead Officer:	Phil Williams, ICT Manager
Statutory Compliance:	- Cyber Crime & Computer Misuse Act (1990) - Data Protection Act 1998 - Human Rights Act 1998 (Right to Privacy)

This page has intentionally been left blank

Title: **ELECTRONIC COMMUNICATIONS & ICT SECURITY POLICY**

1. Introduction

1.1 The continued use of the Internet, electronic communications (both internal and external) and other ICT systems are vital for the Mid-Wales Housing Group's business. However, they also carry serious risks. Careless use of email, social media and the Internet can have serious consequences. For example, it is possible to create a legally binding contract by exchange of email, or 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 the network, infringe copyright laws and result in the harassment or defamation of others. Posting personal opinions on social media sites can have serious implications for both the Mid-Wales Housing Group and the individual(s) concerned. For these reasons, we have to impose security and certain limitations on Internet, email and social media use in relation to both business and personal use. By extension, this also covers the devices by which these services are accessed.

1.2 This policy covers the Mid-Wales Housing Group. The general principles cover all the activities undertaken by the Group. However, there are instances within the policy where the ICT services and configuration of the Care & Repair in Powys Agency are different to those of Mid-Wales Housing Association and this policy has been written to highlight these differences and is based on the current scenario. An action plan will be drawn up to ensure that all of the services are aligned between organisations and then a programme implemented within the ICT Strategy of Care & Repair in Powys to ensure that the additional security options are implemented (budget permitting).

2. Definition Of ICT Security

2.1 ICT Security refers to relevant incidents as well as measures, controls and procedures applied by a company in order to ensure integrity, confidentiality and availability of their data and ICT systems.

3. Policy Statement

3.1 This policy sets out the rules for how our ICT systems may be used (this includes all software applications, the telephone system, fax facilities, laptops, mobile phones, tablets such as the iPad and any internal or external systems they access). It applies to everyone who uses our ICT systems, whether they are used at one of our offices or remotely.

The purposes of this policy are:

- to ensure that all ICT systems, other communication equipment and resources are used correctly and kept secure, including password complexity requirements.

- to establish clear rules on the extent to which email, Internet, social media and telephone facilities (both in the office and remotely) may be used for personal use

- to inform you that monitoring is taking place and the reasons for it

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

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

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 you should seek clarification from the ICT Manager or Human Resources Manager (for Mid-Wales Housing Association) or the Director (for Care & Repair in Powys) before you use any of the ICT systems.

4. ICT System Use

4.1 Hardware Provisions & Security

Desktop PCs, desk telephones, mobile phones, laptops, tablet computers and other shared office equipment such as fax machines, printers and photocopiers have been provided to facilitate office functions, allow access to office software applications, support mobile working arrangements and printing.

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

Within Mid-Wales Housing Group, ICT asset databases (one for each organisation) 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.

4.2 Software Applications & Security

Software applications in use within the Mid-Wales Housing Group are installed on user devices, stored centrally on Server PCs or can be hosted and accessed via the Internet. All of these require some form of identification, be that 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, should be kept secret and not divulged to others (including other staff members).

Security of user logons and passwords for individual user areas and access to software applications is the responsibility of the staff member to whom it was allocated and it must not be used by or divulged to anyone else, other than in accordance with this policy.

4.3 **Unauthorised Operating Systems & Devices**

Mid-Wales Housing Association no longer authorises use of or supports the Windows XP Operating System on PCs or laptops connected to the internal network or for use with remote access to any office systems. This also applies to any Windows operating systems that pre-date Windows XP. These operating systems are now “end-of-life” with Microsoft and are therefore no longer supported or provided with any security updates. This means they are no longer secure on the Internet and therefore should not be connected directly or indirectly to the Internet using any physical or Wi-Fi based networks. Windows XP was made end-of-life by Microsoft in April 2014.

Therefore, any devices still running Windows XP (or earlier versions) should be returned to the ICT Section as soon as possible for evaluation for upgrade to a supported operating system or for secure disposal.

Care & Repair in Powys currently use Windows XP on desktop PCs to host a terminal services connection to the Server. It is recommended that these are upgraded to Windows 7 or higher operating system as soon as possible/practical to maintain security. In the meantime, all of the devices running Windows XP should not be used to “directly connect” to the Internet, but a terminal services connection should be used instead.

4.4 **Web Portals & Cloud Based Storage**

The web portals “Dropbox” and “Google Drive” are permitted for the storage of documentation and for transferring documentation between the Mid-Wales Housing Group and partner organisations (such as Contractors). However, it is not permitted to store any personal data or any company sensitive data/information in these web portals unless the data has been first encrypted with a 256 bit algorithm (AES-256).

Access should be controlled with a frequently changed and complex password (10 characters minimum).

Software applications (such as the dropbox client software) are not permitted for download and installation onto any of the Mid-Wales Housing Group’s Server PCs, Desktop PCs or laptop devices. Dropbox and Google Drive Apps are permitted to be installed onto Apple iPhone/iPad devices.

4.5 **Viruses, Malware & Phishing**

The introduction of a virus or malware into the Mid-Wales Housing Group’s ICT systems could be devastating. These are malicious/unwanted computer programs designed to compromise security or data/information. The ICT section (for Mid-Wales Housing Association) and the Finance/ICT Officer (for Care & Repair in Powys) are 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. You should be aware that viruses and malware can be introduced via email attachments, CD-ROMs, floppy disks, memory sticks and the Internet.

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.

“Fake” communications that pretend to be from 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.

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.

It is the responsibility of each staff member as a 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, please contact the ICT section (for Mid-Wales Housing Association) and the Finance/ICT Officer (for Care & Repair in Powys), who will check whether it is safe to open the attachment. It is not recommended that suspicious emails are forwarded to anyone else (including ICT Administrators), as this could make matters worse, by spreading the potential threat.

“Executable” files attached to emails, stored on CDs, memory sticks or available for download from the Internet, should not be accessed without first obtaining clearance from the ICT section (Executable files can be identified as they have the extensions ‘.exe’, ‘.bat’, ‘com’ or ‘.zip’). If you are in any doubt about an email, a file attachment or Internet download, please contact the ICT section (for Mid-Wales Housing Association) and the Finance/ICT Officer (for Care & Repair in Powys) prior to accessing it.

Staff members should not install or attempt to install any software onto PCs or laptops 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, CD-ROMs, floppy disks or memory sticks without first obtaining the approval of the ICT section (for Mid-Wales Housing Association) and the Director (for Care & Repair in Powys). Mobile devices such as iPhones and iPads can access Apps from the official Apple “App Store” using their issued Apple ID (this also applies to other devices based on Android or Microsoft operating systems). Staff members are permitted to access and download “Free” Apps onto their allocated devices, but must make a request and present a business case to the ICT Manager (for Mid-Wales Housing Association) and the Director (for Care & Repair in Powys) if a chargeable App is required. This would necessitate a credit card to be entered into the Apple account for payment (once complete, the credit card details will be removed).

Within Mid-Wales Housing Association, access to certain web sites is controlled through a web filter which categorises sites (e.g. Drugs, Pornography & News). 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 may incorrectly categorise certain web sites at times. It is also possible that new web sites may not be categorised and be deemed inappropriate. All

instances of this nature should be immediately reported to the ICT section who are responsible for configuring the web filter rules.

Within Care & Repair in Powys, all web sites are accessible and no filtering or blocking takes place.

Devices, connectors, adapters, equipment or media which has not been provided by the Mid-Wales Housing Group should not be connected to any of the ICT systems without prior approval of the ICT section (for Mid-Wales Housing Association) and the Finance/ICT Officer (for Care & Repair in Powys). This includes items such as MP3 players, mobile phones, memory sticks, CDs and DVDs or other devices/accessories that connect via USB ports.

4.6 Cyber Crime & Computer Misuse Act (1990)

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.
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.

The Act recognised the following offences and penalties:

- 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 school or 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.

- 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.

- 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.

- 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 offense 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.

4.7 Wireless Technology

Wireless technology (Wi-Fi) and wireless devices are now commonplace. 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 and also if you should 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	Ask ICT section before attempting connection
Free/Public Wi-Fi networks in coffee shops, libraries etc	Not recommended. If there is no other option, then these can be used to connect using the Citrix Receiver App on iPad devices only, as the connection is “separately encrypted”. No other Apps should be used.

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 or Starbucks). As stated above, the real Wi-Fi networks at these

establishments are not recommended for connection, unless there is no other option available and only then should the “Citrix Receiver” application be used, as it is secure and separately encrypted.

Mobile devices (laptops, mobile phones, tablet PCs) 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 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.

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

4.8 **Travelling/Remote Working/USB Memory Sticks**

Given the amount of confidential information which is accessible remotely, sensible precautions must be taken when mobile devices 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.

Documentation or software systems that contain financial, sensitive or personal details should not be stored locally on any mobile devices, unless they have encryption facilities enabled. 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 Data Protection Act.

Documentation or software systems that contain financial, sensitive or personal details should not be stored on any USB memory sticks unless they are the secure encrypted types and even then their use should be limited. If an unencrypted USB memory stick was lost or misplaced and as a consequence this type of data was released into the public domain it would breach the Data Protection Act.

CD, DVD and Floppy Disk media should no longer be used to store any types of financial, sensitive or personal details whatsoever.

If you are working in a public place, be aware that other people may be able to read documents that you are working on and/or see passwords you are typing in.

When using mobile devices, do not discuss private matters relating to company business or that of our clients and partners if you think you may be overheard.

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.

It is therefore recommended that mobile devices are switched off or set to silent when driving to avoid distractions. The Employment Handbook also clarifies this point.

To reiterate the instruction in point 4.6 above, it is not recommended that remote access is made to any of the Mid-Wales Housing Group's ICT systems using public service internet connections or unsecured wireless networks e.g. Internet cafes, shops, libraries, etc. if other more secure options are available.

4.9 Computer/Device Access Control & Password Policy

The Mid-Wales Housing Group's internal ICT network(s) require that you change your password every 90 days. It is also recommended that all software applications, although not all are mandatory that you do so, undergo a change of password every 90 days (e.g. Covalent, Capita Open Housing/Finance, CARIS).

Passwords should be as complex and random as possible, such that other persons cannot easily guess them. They should not have any association to you (e.g. favourite colour, birth date, car registration, partner or children's names etc). The password policy is as follows, which should be used to select and set your passwords for desktop PCs, laptops and software applications (e.g. Covalent, Capita Open Housing):

Password Length	**Minimum 8 characters (Recommended 10)**
Character Requirements	Should contain a mixture of both upper and lower case letters, numbers and non-alphanumeric characters (e.g "£$%)
Familiarity	The password should be random and not associated to you (favourite word, family member etc)
Change Frequency	Must be changed at least every 90 days
Password Retention	Previously used passwords should not be used again once expired, always choose a new one

Passwords are personal to each staff member and should be kept confidential, not divulged to anyone else, not written down or kept in desk drawers etc. Usernames and passwords belonging to other staff members should not be used by another person to gain access to the Mid-Wales Housing Group's ICT systems, unless there is a pressing business requirement to do so and it has been authorised by an appropriate Director.

Staff members should log out of their allocated desktop PCs when they are not in use or when they leave the office. If leaving the desk for a short period of time, the screen lock facility should be enabled.

All Mid-Wales Housing Association issued Mobile Devices (currently Apple iPhones and iPads) have been configured to require a passcode upon switch on/power up. The screen has also been set to "autolock" after a short idle time. This code is a 4 digit numeric code and must be kept secure and not divulged to anyone else. When you have finished using the device, you must ensure that the screen is locked immediately for security. All of the mobile devices have been configured to erase all contents if the security passcode is entered incorrectly 10 times in succession. The settings that control the passcode, autolock, erase content and find my iPhone/iPad

mechanisms must not be changed or disabled under any circumstances as they maintain the security of the devices. Additional passwords issued with mobile devices (Apple ID, email accounts etc) must also be kept confidential, secure and not stored or kept in paper format with the devices.

All Care & Repair issued Mobile Devices (currently Apple iPads and Nokia Lumia Phones) have been configured to require a passcode upon switch on/power up. The screen has also been set to “autolock” after a short idle time. This code is a 4 digit numeric code and must be kept secure and not divulged to anyone else. When you have finished using the device, you must ensure that the screen is locked immediately for security. All of the mobile devices have been configured to erase all contents if the security passcode is entered incorrectly 10 times in succession. The settings that control the passcode, autolock, erase content and find my device mechanisms must not be changed or disabled under any circumstances as they maintain the security of the devices. Additional passwords issued with mobile devices (Apple ID, email accounts etc) must also be kept confidential, secure and not stored or kept in paper format with the devices.

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

4.10 **Email Security**

It is very easy to send an email to the wrong person. You should be very careful to ensure that the emails you send are correctly addressed, particularly when they contain information that you would not want others to see.

Remember that email is not a secure way of sending information. Emails can be intercepted by third parties and intended recipients can alter and/or forward emails without your knowledge. You should therefore avoid sending by email any personal information about individuals or commercially sensitive information. If the information contained in an email is confidential, you should consider if this is the most appropriate method of communication or ensure the necessary steps are taken to protect confidentiality. Payroll files transferred between organisations using email is a good example where the attached data should be encrypted or transferred via a more secure mechanism.

Care & Repair in Powys have an agreement to encrypt emails between themselves and Powys County Council to protect sensitive data. This encryption should not be disabled or bypassed unless the agreement is changed or terminated.

Remember that deletion from your inbox or archive does not necessarily mean that emails are destroyed, snapshot back-ups are taken and at times we may need to retrieve them. The system also allows retrieval of deleted items for up to 14 days.
Email messages may be disclosed in legal proceedings in the same way as paper documents.

Email access is via a user’s unique network logon, which is password protected or via a user’s mobile device, which is passcode protected. Unauthorised access to email using another member of staff’s logon will result in disciplinary action.

4.11 Email Content

Email should not be used as a substitute for face-to-face communication, when this is deemed necessary or more appropriate under the circumstances.

When sending emails, internally or externally, you should exercise the same care as you would if you were sending a letter on the Mid-Wales Housing Group's headed paper.

Keep messages concise and only copy in individuals who need to see the contents of the email.

You must not send, forward, distribute or retain email messages that contain language that is abusive, aggressive, obscene or offensive. You must not make any improper or discriminatory reference to a person's race, colour, religion or belief system, sex, age, national origin, sexual orientation, disabilities or physique when writing emails and must not forward or distribute any material which does so. Doing so will amount to gross misconduct. The principle should be that you never put something in an email that would offend or embarrass any reader or yourself. Always remember that an email might be seen by someone other than the intended recipient. If you receive any such messages you should inform your line manager or contact the Human Resources section immediately (There is no need to forward or copy an email to someone else under these circumstances, just inform in the first instance). Depending on the circumstances, you may also want to refer to the Employment Handbook.

The effective operation of the network can be hindered when large attachments (such as video clips or pictures, junk mail, hoax virus warnings and e-chain letters) are sent and received. The ICT security systems will filter a number of these incoming communications but you must not send such emails and should ask others not to send them to you for non-business purposes.

Size limits and restrictions have been configured within the email system as follows:

Mid-Wales Housing Association	
Main Mailbox Size	512 Mb
Archive Mailbox Size	2 Gb
File Attachment Size	10 Mb
Email Recipients	100
Malware/SPAM	Potential Message Deletion
File Type Filtering	Potential File Attachment Removal
Deleted Item Recovery	14 days

Care & Repair In Powys	
Main Mailbox Size	2 Gb
Archive Mailbox Size	Not Applicable/No Archive
File Attachment Size	10 Mb
Email Recipients	100
Malware/SPAM	Potential Message Deletion
File Type Filtering	Potential File Attachment Removal
Deleted Item Recovery	14 days

These limits may be varied at the discretion of the ICT Section/Director of Care & Repair in Powys but good 'housekeeping' prevents the overloading of mailboxes. The majority of problems with mailbox size are due to file attachments; these should be removed from emails and stored in the relevant file system.

Please note that within Mid-Wales Housing Association Main Mailboxes automatically decant all content over 6 months old to the Archive Mailboxes. Both mailbox structures are accessible to users and as both have imposed size limits, both must be maintained on a regular basis to avoid warning messages or mailbox suspension due to reaching the imposed limits. There are no Archive Mailboxes within Care & Repair in Powys so all items remain permanently in the Main Mailbox unless deleted.

A Mid-Wales Housing Association auto-signature within the email client software (currently Microsoft Outlook) is set as a default by the ICT Section but can be amended by employees as appropriate. A default company email disclaimer is also automatically stamped to all outgoing emails. This is a legal requirement, which acts exactly the same as a company letterhead.

A Care & Repair in Powys auto-signature can be set and amended by employees within the email client software (currently Microsoft Outlook). A default company email disclaimer is also automatically stamped to all outgoing emails.

It is possible to create legally binding contracts without intending to via email correspondence. Email must not be used for communications that could lead to a binding contract being formed or which would have the effect of obligating the company in any way, unless you have the clear authority to make the commitment in question. Remember, a typed name at the bottom of an email is the same as a signature on a letter.

Any complaints from tenants, clients, business contacts or any other source, received via email, should be forwarded immediately to the Performance Officer (for Mid-Wales Housing Association) or the Director (for Care & Repair in Powys).

4.12 **Calendars**

The Mid-Wales Housing Group operates an open calendar policy. This means that all staff members have the ability to view the calendar of all other users. Calendars provide the ability to create meetings, invite other staff members and check their availability. Rooms can also be booked at the same time. When making entries/appointments in your calendar it is important that you describe the subject

matter in appropriate and discreet terms, bearing in mind that it can been seen by all staff members (using the default settings).

An option is available to change the setting of a calendar appointment and mark it as “private”. This setting means that the entry/appointment is only visible to the creator and any requested attendees.

Staff members are allowed to make calendar entries for personal appointments but the subject will be visible to others, unless you have marked it as “private”.

4.13 Copyright

Most information and software that is accessible on the Internet is subject to copyright or other intellectual property protection. Nothing should be copied or downloaded from the internet for use within the company or on our equipment unless the owner of the material has given express permission.

4.14 Personal Use

The Mid-Wales Housing Group’s ICT equipment and systems are to be used solely for business purposes, subject to the following exceptions:

- You may make reasonable use of Mid-Wales Housing Group’s ICT systems for personal emails, as long as this is done outside normal working hours or during the lunch break, in accordance with the terms of this policy.

- You may make reasonable use of Mid-Wales Housing Group’s ICT systems for Internet access (including social media), as long as this is done outside normal working hours or during the lunch break, in accordance with the terms of this policy. For further information on the approved use of social media, please refer to Mid-Wales Housing Group’s Social Media Strategy & Policy documents.

- You may make reasonable personal use of the Mid-Wales Housing Association’s mobile devices and connect them to home Wi-Fi networks, as long as you comply with the signed usage agreements, security requirements and your usage does not impact on any of the Mid-Wales Housing Group’s usage contracts with mobile network providers. Personal usage that is extra to these contracts (data usage, voice calls and SMS texts) will be recharged to the individual staff member(s). This includes excessive personal usage, calls to premium lines, calls to chat lines, overseas calls and international roaming.

- You may make occasional private/personal calls using of Mid-Wales Housing Association’s telephone systems, as long as this is done outside normal working hours or during the lunch break, in accordance with the terms of this policy. Personal calls to premium lines, calls to chat lines and overseas calls are never permitted.

- Within Care & Repair in Powys personal use of the telephone system and mobile phones is permitted only in an emergency.

4.15 Monitoring Communications

We log and audit the use of:

- Telephones, mobile devices and fax machines
- Computers, laptops and mobile devices including email, Internet and other computer use
- Personal mobile telephones and landlines if we pay for them or contribute towards their cost

Within Mid-Wales Housing Association, all telephone calls from all extensions (inbound and outbound) are logged and regularly audited. Auditing software has been installed to monitor any Internet sites visited. We keep back-up tapes that record computer usage which are retained in accordance with data protection legislation.

Within Care & Repair in Powys, telephone calls are not logged but are itemised on monthly bills. Internet sites visited are not logged or audited currently.

Company mobile device contracts provide the Mid-Wales Housing Group with itemised usage logs/reports. These are regularly monitored and any excessive usage or personal usage that is extra to the standard contracts is recharged to individual staff member(s).

Where we have good reason, we may monitor and record the contents of telephone calls, voicemail messages, faxes, computer files, Internet use and emails sent, received and stored. We will always act within the law. You should also be aware that your emails and voicemails may be checked during times when you are absent from work. Given this, you should not regard either business or personal communications as private.

Within Mid-Wales Housing Association, telephone calls made from the internal telephone system (currently Avaya Communications Manager) are restricted on a handset basis by “class of service” as follows:

- Directors, ICT Manager - Unrestricted Access
- Managers/Team Leaders - Premium Rate Numbers Barred
- All Other Staff Members - International & Premium Rate Numbers Barred

Within Care & Repair in Powys, telephone calls made from the internal telephone system (currently Siemens OptiPoint 500) are not restricted by handset or by class of service.

4.16 Purposes Of Monitoring

The purposes of such logging, auditing, monitoring and recording are to:

- Ensure the effective operation of our ICT systems and to maintain system security, including the retrieval of lost messages
- Investigate and detect unauthorised use of the systems in breach of this policy, such as excessive personal use or distribution of inappropriate material.
- Check whether any matters need to be dealt with in your absence
- Investigate allegations of misconduct, breach of contract, a criminal offence or fraud by the user or a third party
- Pursue any other legitimate reason relating to the operation of the business.

This list is not exhaustive.

The information gathered will only be given to those who need to see it in accordance with these purposes. If information gathered is relevant to any disciplinary action taken, it will be made available to those who are involved in the disciplinary procedure.

4.17 Social Media

Social Media should be broadly understood to include blogs, wikis, message boards, forums, chatrooms and popular sites such as Facebook, Twitter, Instagram, LinkedIn etc.

Personal use of Social Media has been discussed previously in this document. Also has the reference to additional information that can be found in the Mid-Wales Housing Group's Social Media Strategy & Policy documents.

The principle contained within this document regarding viruses, malware, phishing and general security also apply to social media:

- Passwords should be complex, not based on familiar words or phrases, not written down and should be kept secret
- Viruses and malware can come through social media sites, so care should be taken when accessing downloadable files and links to other sites or content.
- Phishing attacks can also take place within social media, therefore requests for confidential or personal data should always be treated with caution and should be assessed for authenticity (by other means) before being accessed on social media.
- Personal or confidential information relating to Mid-Wales Housing Group's business, staff or clients should not be posted onto social media

It is the responsibility of each staff member as a user, to take care when accessing social media. If there is any doubt about a social media site, the information presented or requested, please contact the ICT section (for Mid-Wales Housing Association) and the Director (for Care & Repair in Powys) for further assistance.

5. Disposal Of Equipment & Secure Destruction Of Data

5.1 Disposal Of Equipment

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 order of preference, as follows:

1. Where possible the equipment should be reused in another section/department/member organisation of Mid-Wales Housing Group.

2. Consideration should be given to donating the equipment to local charity or community projects for reuse.

3. The equipment can be sold or donated to Board Members, Staff Members or other outside organisations, subject to Mid-Wales Housing Group's financial guidelines (and the residual value of the equipment to be disposed).

4. The equipment should be recycled or disposed of in an environmentally-friendly manner using Mid-Wales Housing Group's current specialist equipment secure disposal/data destruction organisation Keycom Plc.

5. Where disposal is outside of the Mid-Wales Housing Group, this requires the approval of the Director of Finance (for Mid-Wales Housing Association) or the Director (for Care & Repair in Powys) and must be done in adherence with the Financial Regulations.

ICT Systems that have been installed within the Server/Comms Room, such as Server equipment, telephone systems and hard-disk arrays that are responsible for storing secure or confidential data, should never be donated or passed on to other organisations or individuals. These should always be securely disposed by Mid-Wales Housing Group's current specialist organisation Keycom Plc.

ICT equipment will be sold at a value considered reasonable by the ICT Manager/Director of Finance (for Mid-Wales Housing Association) or the Finance/ICT Officer/Director (for Care & Repair in Powys) and this will take into consideration:

- The approximate market resale value

- The general age and condition

- That the equipment is "sold as seen", without warranty, support, software or services of any kind.

5.2 Secure Destruction Of Data

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 Data Protection Act.

Ensuring adequate destruction of data is the responsibility of the ICT Manager (for Mid-Wales Housing Association) or the Director (for Care & Repair in Powys) and must not be delegated to any other person(s) without adequate contractual obligations being imposed.

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.

All hard disks that are to be disposed of and not reused should be physically dismantled and destroyed. In the case of Server equipment, this should be completed by a specialist organisation (currently Keycom Plc).

Other forms of media, such as CD, DVD, Floppy Disks, ZIP or USB flash drives and data tapes should never be sold or donated to any other organisation or individual, but always be physically destroyed, preferably by a specialist organisation (currently Keycom Plc).

Mobile phones or tablet computers such as the iPad or iPhone, if they are to be sold, donated or 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).

6. Managing Configuration Changes, Updates & Upgrades

6.1 Change Control

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:

Mid-Wales Housing Association	
Change Requested	**Approval/Authorisation Required**
Changes to Active Directory Users or groups	Line manager authorisation
Changes in access to group/public folders	Line manager authorisation
New user addition/removal	Notification from HR Section
Changes to Covalent security access or Action, PIs & Risks responsibility	Line manager authorisation
Changes to Covalent PI configuration,	Performance Management Team

data, targets or tolerances	
Changes to Covalent Risks	The member of Executive Group to whom the risk has been assigned or the Chief Executive
Changes to requisition, authorisation and purchasing levels in Capita Open Housing/Finance	Finance Manager, Executive Group
Changes to Capita Open Housing/Finance security groups	Line manager authorisation
Changes to any ICT hardware or security mechanism (e.g. Telephone System, Internet Firewall)	ICT Manager
Changes to Capture IT or Vizual Personnel user configuration	HR Manager
Changes to Office access control	HR Manager or ICT Manager
Access to another users mailbox or send on behalf of permissions	The mailbox owner, relevant member of or Executive Group (by department) or the Chief Executive
Access to blocked websites	Staff member request, but at the discretion of the ICT Manager
Access to blocked email file attachments	Staff member request, but at the discretion of the ICT Manager
Other request/security change	Initially the ICT Manager, but may also require Executive Group approval dependant on the request
Recovery of deleted files from group, public and home folder storage	Staff member action, but recommended that assistance be first sought from the ICT Officer or ICT Manager
Recovery of deleted mailbox items	Staff member action, but recommended that assistance be first sought from the ICT Officer or ICT Manager

Care & Repair In Powys	
Change Requested	**Approval/Authorisation Required**
Changes to Active Directory Users or groups	Director authorisation
Changes in access to group/public folders	Director authorisation
New user addition/removal	Notification from the Director
Changes to CARIS security or configuration	Director authorisation
Changes to Sage Accounts security or configuration	Director authorisation

Changes to any ICT hardware or security mechanism (e.g. Telephone System, Internet Firewall)	Director authorisation
Changes to Office access control	Director authorisation
Access to another users mailbox or send on behalf of permissions	The mailbox owner or the Director
Access to blocked email file attachments	Staff member request, but at the discretion of the Director
Other request/security change	Director authorisation

6.2 Updates, Upgrades & Implementations

All ICT network level configuration changes are subject to the following approval/authorisations:

- 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 ICT Manager/Director of Finance (for Mid-Wales Housing Association) or the Director (for Care & Repair in Powys).

- All software or firmware version updates or upgrades must first be approved/authorised by the ICT Manager/Director of Finance (for Mid-Wales Housing Association) or the Director (for Care & Repair in Powys).

- Within Mid-Wales Housing Association, all Microsoft monthly security patches and service packs must be approved and released for installation by the ICT Officer, ICT Manager (or the Director of Finance). Within Care & Repair in Powys these are automatically approved by the Server and under normal circumstances require no additional user intervention.

- All other security patches and service packs must be approved for installation by the ICT Manager/Director of Finance (for Mid-Wales Housing Association) or the Director (for Care & Repair in Powys).

- All recoveries of files, software applications or Servers from backup storage (deduplication store or tape) must be first approved by the ICT Manager/Director of Finance (for Mid-Wales Housing Association) or the Director (for Care & Repair in Powys)

- All software and hardware installations/implementation projects must first be approved by the ICT Manager/Director of Finance (for Mid-Wales Housing Association) or the Director (for Care & Repair in Powys).

- All other network level configuration changes that are not specifically listed above should be notified to the ICT Manager/Director of Finance (for Mid-Wales Housing Association) or the Director (for Care & Repair in Powys) for approval.

7. Your Right To Access

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

8. Review

The Mid-Wales Group's electronic communication & ICT security policy will be **reviewed every three years** to ensure its on-going relevance.

Strategic Risk Factors	- Failure to keep up with technological advancement (SR14/025). The world of ICT Security is fast changing and every measure should be taken towards keeping pace with the changes, ensuring all security products/services are current and not outdated and become a potential security risk.	
Equality Impact Audit	*How does/will this policy ensure needs are met fairly, particularly with regard to race, gender, disability etc?*	This policy covers ICT Security mechanisms in place to protect all individuals using the system. As long as specific needs are met in the way of general usage and accessibility (in the instance of disability), then security should pose no additional burden than that of standard usage.
	Is it felt that this Policy might affect different groups adversely. If so what is the justification for this, and is it legally permissible?	Not Applicable
	Have any representative groups in the locality been asked for their opinion and if so what was the outcome?	No
Tenant Engagement	*How does/will this policy ensure the needs of tenants are met?*	Before this policy was drafted, a consultation exercise was held with members of T&RF on 03/10/2014.
	How is it felt this Policy will impact on the rights and obligations of tenants?	It does not. The policy has been written for staff members. However, the principles of ICT security within the document, if applied, would be of benefit to tenants.
	Have tenants been consulted and were the outcomes of that consultation taken into account when considering the introduction of this Policy?	Yes. A consultation exercise was held with members of T&RF on 03/10/2014. The previous policy was discussed in detail. Nothing specific was raised that would alter the policy in great detail. The majority of comments received were to clarify understanding, therefore different language has been used where possible within the policy to make technical aspects clearer and easier to understand.