WILLIAMSBURGH
HOUSING ASSOCIATION

INFORMATION SECURITY & ACCEPTABLE USE POLICY

Revision History

Revision Date	**Reviewer(s)**	**Review Date**	**Description of Revision**
Oct 2022	Finance and IT	Oct 2024	Consolidation of the following policies: ➢ Information Security and Acceptable use of ICT policy ➢ Laptop & iPad policy ➢ Portable Devices & Removable Media policy Update of clause 2.2.4 Clear Desk policy and 2.6 Home working. Update to Appendix 2 of Data Protection Policy

This policy can be made available in different languages and other formats such as Braille, large print or tape, on request.

Contents

Appendices:

1. Summary

The Information Security & Acceptable Use Policy (IT policy) applies to all Williamsburgh Housing Association ("WHA") employees, committee members, contractors and agents (hereafter referred to as "individuals").

Information security is of great importance to WHA. The policy is designed to protect all information handled by the Association, protect all individuals and provide a framework for information security policies.

The policy ensures:

- Maximum safeguard from security threats
- Integrity of information is maintained by protection from unauthorised modification
- Confidentiality of information is maintained
- Compliance with legislation (e.g., United Kingdom General Data Protection Regulation (UK GDPR, Computer Misuse Act.)
- Clear guidance of acceptable use of systems and information for all individuals
- This Policy should be read in conjunction with WHA's Data Protection Policy and associated procedures.

This policy is mandatory and all individuals with access to WHA's systems are required to read this policy and complete annually a declaration confirming understanding & compliance with this policy (See appendix 1).

This policy does not set out to restrict unneccessarily but rather encourage individuals to make use of electronic communications, in a safe and secure manner. The many threats to modern technology make it vital to closely regulate our actions and protect important data, the reputation of WHA, our staff and above all, our customers.

Individuals with questions, concerns or comments concerning this policy or the use of electronic communications generally, should consult their line manager or Finance & IT Manager.

Any breaches of security & non- compliance with this policy must be reported to the Finance & IT Manager or IT Officer immediately using the incident form (Appendix 2). Note, breaches may result in disciplinary action being taken against the individual.

2. Requirements

2.1 Network Security and Wi-fi access

2.1.1Network access

Only Williamsburgh Housing Association owned Laptops, PC's & iPads are allowed to be connected to WHA's network.

Mobile working and bring your own device at work are covered in more detail in Section's 2 & 4.

2.1.2 Physical Access

Access to data held on WHA information systems is minimised by restricting physical access to the WHA office.

Access to Servers and related equipment is restricted by placing in lockable cabinets with keys held in key safe in separate location.

Where information is kept in WHA's office, access to buildings is restricted by ensuring that security doors are closed properly and that entry codes are kept secure.

Doors and windows must always be secured when the office is left unattended.

Visitors to the Associations Office must be signed in and out of the premises on arrival and departure.

2.2 Computer Security

2.2.1 Laptops/iPad/Smartphones/

Laptops/iPads must be kept in a secure location when not in use as individuals are responsible for the safekeeping and security.

Computer equipment or manual files that are travelling with an employee must be locked in the boot of the car and not left overnight. They must always be kept with the individual when travelling by public transport.

iPads and Smart Phone devices must be protected with a password or PIN Number to protect the device and any stored data.

WHA issued mobile devices are for work-related purposes only (if used for personal use, WHA must be reimbursed for call charges including VAT.

2.2.2 Data Storage

All staff must abide by the rules of the UK GDPR and the Computer Misuse Act.

Storage of data should not be held on PC or Laptop’s C: drive (including desktop) as these drives are not included in the nightly back-ups.

Sensitive data should not be stored on portable devices or media.

The following types of files can only be stored if they relate to business needs.

File Type Description

AVI Movie Files / MPG Movie Files / MPEG Movie Files / MP3 Sound Files
MP4 Sound Files / M4A iTunes Files / MOV Movie Files / SCR Screen Savers

EXE Executable files – Used for installing software. NO individuals other than the IT Officer/IT Assistant are permitted to installing software.

2.2.3 File Storage and Naming Conventions

All documents should be given clear and descriptive titles and saved in suitably named folders.

Information which is no longer required (in line with WHA’s document retention schedule) and to comply with the UK GDPR, should be promptly disposed of by deletion or destruction.

2.2.4 Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, WHA enforces a clear desk and screen policy as follows:-

All personal, sensitive or confidential information must be handled with care and stored securely.

Computers must be logged off/locked or protected when unattended (Windows Key + L locks the PC). VPN or LogMeIn sessions should be disconnected, and staff must sign out of all equipment at the end of the working shift

Care must be taken to not leave confidential material on or around photocopiers.

All private and confidential business-related printed matter must be disposed of using confidential waste bins provided throughout the office.

2.2.5 Memory Sticks and removable media

Only WHA supplied encrypted memory sticks are to be used.

WHA memory sticks that have been in use outside the office must be Virus checked by IT before being used on WHA computers.

No data should be transferred to a home PC / Laptop.

2.2.6 Passwords

Passwords must be protected appropriately (do not write passwords down or give them to other users). Do not use personal passwords for logging onto WHA systems.

Passwords should be complex and consist of the following.

At least 16 alpha-numeric characters
Uppercase/Lowercase
At least 1 number
At least 1 Special Character

If you think your password may have been compromised, change it immediately and report it to IT.

If your manager needs access to your computer whilst you are off sick, they must contact the Finance & IT Manager or IT Officer to request a password reset.

2.2.7 Viruses and other threats

The main threats to WHA system's are viruses from e-mail attachments, files/programmes downloaded from the internet, individuals installing their own software and removable media i.e. dvds or usb drives. All WHA's computers have pre-installed anti-virus software which is continually updated with the latest known virus profiles.

All files received on portable media from outside WHA or received via electronic mail must be checked for viruses before being used on WHA equipment. You must not intentionally introduce/send or download files or attachments which contain viruses into WHA's systems.

If a virus is suspected, the IT department must be informed immediately. The workstation should not be used until given permission from the Finance & IT Manager or IT Officer and a sign stating this should be placed on the workstation to warn other users. Any disks, DVD's, and USB memory sticks that have been used on the suspected infected workstation should be gathered and not used.

2.2.8 Ransomware

Ransomware attacks are all too common these days and Ransomware has attacked organisations in nearly every size.

Ransomware is a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the victim pays a fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever.

Individuals should be aware of clicking on links in emails from strangers or opening email attachments. If in any doubt the emails should be deleted.

Individuals should also be aware of any popups on devices where it asks you to click on link to take you to unknows websites.

2.2.9 3rd Party Network Connections and Administrator Level Access

All requests for external 3rd Party network connections must be processed by the Finance & It Manager or IT Officer and will be strictly governed by relevant standards.

Administrator Level access is restricted to IT Officer, IT Assistant and Chess ICT Support. Where it is deemed necessary to give administrator level access to 3rd Parties, the Administrator Access Level Request form must be filled in and reviewed by Finance and IT Manager and IT Officer.

Administrator Level Access must be removed immediately it is no longer required and details updated on the Administrator Level Access form.

2.2.10 Printing & Scanning

Individuals must ensure adequate care is taken when printing & scanning information. If there is a printer fault when printing OFFICIAL or SENSITIVE material, please contact the IT department who will delete any unprinted files from the print queue. When scanning, individuals must ensure adequate care is taken to check destination file/email address.

Personal use of network printers is not disallowed by this policy and is permitted if this does not interfere with the performance of expected duties. Usage time should not be excessive and should be restricted to personal time, as far as possible.

2.2.11 Lost or stolen mobile devices

If a mobile device is lost or stolen, staff must:

- Contact the IT Officer or IT Assistant on 0141 847 6378 or 0141 847 6377 to report the loss and ask for the mobile device to be suspended so that it can no longer be used.

- Complete a Report on an Information Security Incident form. (Appendix No. 2.)

- Notify the local Police station of the loss.

Please note that replacement of lost or stolen handsets is not covered by any insurance so WHA will need to pay for the replacement.

2.2.12 Leaving WHA or moving into another role

Staff who are leaving WHA must ensure safe return of all WHA equipment.

2.3 Use of the Internet

2.3.1 Downloading of Information Resources

Individuals must not download non-work-related information from the Internet. To reduce the likelihood of a virus infection, individuals must take care to ensure that work related files are from a trustworthy source.

Individuals requiring any new software, including any plug-ins, must make a formal request to the Finance & IT Manager or IT Officer.

Software must not be downloaded and/or installed onto WHA's equipment unless it has been approved by the Finance & IT Manager or IT Officer and can be validated that it is licensed for current use.

Graphical, audio and video files may be downloaded and stored on WHA network for business use only.

Individuals are reminded that copyright laws apply to the Internet and care must be taken should there be a need to re-use any information (including images) in any Association work.

2.3.2 Uploading Data / Information to the Internet

Any users who are responsible for uploading data / information to the Internet must be sure that the information being uploaded is suitable to upload, and not SENSITIVE or OFFICIAL.

2.3.3 Internet Filtering and Blocking

Users should not attempt to by-pass WHA's Internet filtering software.

Staff who encounter a commonly used business site which is blocked and have genuine business reasons for accessing that site should contact the IT department and request the site is on an approved list of websites.

2.4 E-mail Use

WHA's email platform is Microsoft Outlook 365 and should not be used for non-work-related matters.

2.4.1 Sending email

External e-mail messages should have appropriate signature files as updated periodically from WHA and should have the following disclaimer attached:

> "Williamsburgh Housing Association Ltd is a recognised Scottish Charity no.SC 035350. Confidential Disclaimer Statement This message and any associated folders is strictly confidential and may be privileged. It is intended solely for the person(s) or organisation to which it is addressed. It may contain confidential material protected by copyright or which constitutes a trade secret. If you are not the intended recipient, you are hereby notified that any dissemination or copying of this message, or folders associated with this message, is strictly prohibited. If you receive this e-mail in error, please delete it and notify Williamsburgh Housing Association immediately. It is the responsibility of the recipient to ensure that the onward transmission, opening or use of this message and any attachments will not adversely affect their systems or data. This message has been scanned with Sophos Anti-Virus and has been certified as virus free when it left Williamsburgh Housing Association. Please carry out all virus and other checks as appropriate".

2.4.1 Sending email cont.

This disclaimer is added automatically and must never be altered or deleted. Individuals should immediately inform the Finance & IT Manager or IT Officer if this information does not appear on their e-mails.

Confidential or sensitive information such as special category personal data should not normally be sent by e-mail (unless it is encrypted). If unsure, individuals should check with their manager,

All e-mails must have the subject line completed and should be checked for accuracy of spelling, punctuation, and grammar.

Before sending emails, a check should be made to ensure you are sending to the correct recipient. Sending emails to the wrong email address may result in a UK GDPR data breach. (All breaches should be reported to the WHA Data Protection Lead immediately).

Individuals must not alter the text of any received messages, including when forwarding them to others. Similarly, individuals should not assume that a forwarded message matches what was originally authored.

2.4.2 Agreements by email

Individuals must take care not to enter into any agreements via e-mail that could constitute a contract, and if in doubt must seek the advice of your line manager.

2.4.3 Mailbox size and housekeeping

The standard individual mailbox size provided by Microsoft Outlook 365 is 50 GB. Each mailbox will have a designated owner who will be responsible for housekeeping (archiving or deletion) all types of Microsoft Outlook 365 items. Once the mailbox limit is reached, users of that mailbox will not be able to send or receive any further mail and therefore housekeeping must be planned well in advance of reaching the space limit.

2.4.4 Distribution lists

Mail distribution lists are provided to enable business communications to be made to groups of individuals. Lists should only be used for related business purposes.

To comply with UK GDPR, you should use blind carbon copy to stop personal details being sent to other recipients on your distribution list. (All personal data breaches should be reported to the Data Protection Lead immediately).

2.4.5 Mailbox management

Individuals are expected to treat their mailbox like an electronic in-tray, ensuring that it is regularly checked and that messages requiring further action are dealt with promptly – including sending holding responses where appropriate.

Individuals should only archive and retain messages that need to be kept and these should be selected in line with business needs and any corporate retention schedules that may exist. All other e-mail that does not constitute a necessary record of business should be deleted once it is no longer required.

When an email is received with an attachment which needs to be retained, individuals should save the attachment to the departmental network drive, and not leave the attachment within the email.

2.4.6 Misuse of email

Individuals must not send or forward any abusive, threatening, defamatory or obscene messages. Likewise, individuals should avoid sending messages in the heat of the moment, taking time to reflect on drafts and how they may be interpreted before sending them.

Individuals must take care with any suspected malicious or nuisance e-mails received (e.g., phishing, hoax and spam e-mails) and delete them.

If any suspicious e-mails are received, they should be reported to the IT Officer or IT Assistant.

Individuals must never open attachments to an e-mail of unknown origin as they may contain viruses and other malware.

Never respond to an e-mail requesting personal details.

2.4.7 Mail and absence

An "Out of Office" notice must be used when an individual is away from their normal base, and messages should clearly indicate a date of return and contact details for those who can deal with issues whilst the individual is away.

2.4.8 Attachments

Attachments should not be included in any internal mails or meeting invites, wherever it is possible links to documents should be used instead.

2.5 Office Telephones

Individuals are expected to use the telephone for the duties they are employed to undertake. WHA recognises, however, that sometimes it is necessary and reasonable for employees to use the telephone for personal calls. Individuals are, therefore, allowed to make and receive short personal calls, if they are necessary, reasonable, and small in number.

2.6 Home Working

Staff who work from home are required to comply with all IT security and confidentiality requirements of WHA. You must follow WHA's policies and procedures in relation to working with personal data as if you were still based in the office. The data protection principles still apply and need to be adhered to, ie, you should only access personal data that is needed for "specified, explicit and legitimate purposes". You should "limit what you take home to only what is necessary" and keep it there for "no longer than is necessary".

The home worker will have a direct responsibility for all WHA information material held at their home and must ensure that it is not accessible to non-authorised people (e.g., other members of the household).

Staff working on WHA business at alternative work sites must use WHA provided computer and network equipment unless other devices have been approved by the IT Officer or IT Assistant.

Staff must not use their own mobile computing devices, computers, computer peripherals, or computer software for WHA business processes. All remote access to WHA networks must be made through approved Remote Access methods that are controlled by the IT department.

After a remote worker has completed a remote session with WHA systems staff must disconnect the remote session and log off their PC/laptop. Under no circumstances should a remote session be left open when the user is away from their PC/laptop for an extended period.

The display screens for all systems used to handle WHA sensitive information must be positioned such that they cannot be readily viewed by unauthorized persons through a window, over a shoulder, or by similar means.

Remote workers must not share passwords or any other access devices or parameters with anyone without prior approval from the IT department. This means that a remote computer used for WHA business must be used exclusively by the member of staff. Family members, friends, and others must not be permitted to use WHA equipment.

All computers used for remote working (including portables, laptops, notebooks, and other transportable computers) which contain confidential or sensitive WHA information must consistently employ both hard disk encryption for all data files and start-up protection through a password.

2.7 Home Printing

Staff should take particular care that any confidential information, or documents containing personal data, are disposed of correctly. If an individual does not have access to a shredder, then documents should be held securely until such time as they can be disposed of correctly.

2.8 Chat programs

Chat programs are for informal business use only (e.g., Microsoft Teams) and must not be used to convey any personal information (e.g., tenants names, phone numbers email addresses etc. to other members of staff.

3. Wi-Fi Connections

3.1.1 Office Wi-Fi Connections

Internet access from mobile devices for staff, committee or any external visitors should be via the ‘WHA Guest Wi-Fi’ wireless network only.
Under no circumstances should any non WHA device be allowed access to the network with the use of a network cable.

3.1.2 External Wi-Fi Connections

It is important that only secured Wireless (Wi-Fi) connections are utilised. These connections are typically announced as, and secured by, WPA/WPA2.

The following connection types are not permitted:

WEP (wired equivalent privacy) secured – known to be insecure; easy to gain unauthorised access to the network.

Public Hotspots- These should be avoided due to the uncertainty of the security of the provided network.

Certificate Errors – If a certificate error is displayed upon connection, then your device should be disconnected immediately and an alternative Wireless access point found, as the security of the connection cannot be guaranteed.

4. Bring Your Own Device to Work (BYOD)

WHA does not allow individuals to use equipment not supplied by WHA. However, one exclusion to this, is using personal mobile phones to access WHA email (and data contained within).

WHA, as the data controller, remains in control of the data regardless of the ownership of the device. Users are required to keep any information and data belonging to the WHA securely. This applies to information held on a user’s device, as well as on WHA’s systems.

Users are required to assist and support WHA in carrying out its legal and operational obligations, including co-operating with the IT department should it be necessary to access or inspect data belonging to WHA stored on a device.

WHA reserves the right to refuse, prevent or withdraw access to users and/or devices or software where it considers that there are unacceptable security or other risks including but not limited to its staff, employees, business, reputation, systems, or infrastructure.

4.1 System, Device and Information Security

The use of a user's device must adhere to WHA's policies regarding security and compliance with data protection law.

Where an individual uses a device as a work tool, users must maintain the security of WHA's data and information which a user processes (which includes, but is not limited to, viewing, accessing, storing, or deleting information and data (in emails) belonging to WHA).

It is the individual's responsibility to familiarise themselves with the device sufficiently to keep data secure. In practice, this means:

preventing the theft and loss of data
keeping information confidential, where appropriate; and
maintaining the integrity of data and information.

Individuals must never retain personal data from WHA's systems on their device. If individuals are in any doubt as to whether data can be stored on a device, they must err on the side of caution and consult their manager or seek advice from the IT department.

Individuals must always:

- use the device's security features, such as Biometric, PIN, password or passphrase and automatic lock to help protect the device when not in use.

- keep the device software up to date, for example Apple iOS or Android updates

- activate and use encryption services and anti-virus protection if user's device features such services.

- install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone app', Androids 'Where's My Droid' or Windows 'Find My Phone', where the device has this feature.

- remove any information and data belonging to WHA stored on an individual's device once a user has finished with it, including deleting copies of attachments to emails, such as documents, spreadsheets and data sets.

- limit the number of emails and other information that users are syncing to the device to the minimum required, for example only keep the past 24 hours of email in sync.

- upon leaving WHA, the device owner must allow the device to be audited by WHA to ensure all WHA Data has been removed.

4.2 Loss or Theft

If a device is lost or stolen, or its security is compromised, this is a security incident and individuals must use Appendix 2 incident form to report this to the IT department immediately. Any passwords giving access to WHA systems will then be changed.

It is also recommended that users also do this for any other services that have been accessed via that device, e.g., social networking sites, online banks, online shops). Users must also cooperate with the IT department in wiping the device remotely, even if such a wipe results in the loss of User's own data, such as photos, contacts, and music.

WHA will not monitor the content of user's personal devices. However, the IT department reserves the right to monitor and log data traffic transferred between a user's device and WHA systems.

4.3 Access to personal device

In exceptional circumstances, for instance where the only copy of a document belonging to WHA resides on a personal device, or where WHA requires access to the device to comply with its legal obligations (e.g., it is obliged to do so by a Court of Law or other law enforcement authority) WHA will require access to data and information owned by the WHA stored on a User's personal device. Under these circumstances, all reasonable efforts will be made to ensure that WHA does not access Individual's private information.

Individuals are required to conduct work-related, online activities in line with WHA's policies and procedures.

4.4 Support

WHA takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding BYOD devices.

4.5 Use of Personal Cloud Services

Personal data as defined by the Data Protection Act 2018, UK GDPR, confidential information, and data belonging to WHA may not be stored on **personal** cloud services (e.g., One Drive / Dropbox etc.)

5. Controls and Responsibility

The senior management team must ensure that individuals adhere to this policy. IT staff will be responsible for monitoring systems under their control for signs of:

- Illegal or unauthorised software having been loaded
- Password misuse
- Unauthorised access

If you have any questions about this policy, in the first instance, speak to your manager.

Managers must fill in a "New User Network Access" form to ensure that new staff who require access to IT are provided with log-in credentials and access privileges as appropriate. Appendix No. 3.

Managers must also take responsibility to ensure:

All new staff receive a briefing on this policy as part of their introduction to WHA and formally sign the "Acknowledgement of Acceptance" before they are given access to any of WHA's Systems.

All individuals must review this policy and re-confirm acceptance on an annual basis or when invited to do so.

Managers must submit a "Leavers Form" to the IT department who will ensure that the leavers IT account is closed immediately.

Individuals must ensure all IT equipment is returned to the IT department before leaving the organisation.

Managers must ensure that the users work related information, e-mails and data is transferred, if required, to the respective working directory for future access on the system or is deleted. This will ensure that the appropriate security is maintained on leaver's information and data.

6. Privacy

Whilst WHA will not monitor the contents of mail messages as a routine procedure, it does reserve the right to inspect, copy, store and disclose the contents of electronic mail messages, at any time. It will only do so, however, when it believes it is appropriate, to prevent or correct improper use, satisfy a legal obligation, or ensure proper operation of the electronic mail facilities. Where it is considered that such scrutiny is necessary, the prior approval of the CEO (or in his absence, equivalent person) must be obtained.

Some individuals within WHA, by virtue of their positions or specific responsibilities may, in the normal course of doing their assigned work, have special access privileges to hardware and software and, therefore to, the content that resides in those resources. WHA will strive to protect individual privacy by ensuring that the number of people with this level of access is limited.

7. Policy Review

This policy will be reviewed every two years. We will continue to monitor and evaluate any new threats to the security or integrity of data as well as adapting to new technologies and legislation requirements.

Appendix No.1

Staff Declaration:

ACKNOWLEDGEMENT AND ACCEPTANCE

I have read and understand Williamsburgh Housing Association's Information Security & Acceptable Use Policy and agree to be bound by the terms as set out.

NAME: ______________________________

POSITION: ______________________________

DEPARTMENT: ______________________________

SIGNATURE: ______________________________

Please return signed declarations to your line manager.

Appendix No. 2

Security Incident Reporting Form

Your Details	
Your name:	
Your phone number:	
Your contact email address:	
Organisation Details	
What organisation are you reporting for?	
What is your role?	
Incident Details	
Summary of incident:	
Investigation so far:	
Impact:	
Description of impact:	
Current state of incident:	
Additional Information:	

Who else has been notified:
Have you reported this to the WHA Data Protection Lead as a UK GDPR obligation?
Do you have any further data or samples to aid this incident?

NAME: ____

POSITION: ____

DEPARTMENT: ____

SIGNATURE: ____

DATE: ……………………………………………………………………………

Appendix No.3

APPLICATION FOR NETWORK ACCESS/REMOVAL

PLEASE ALLOW A MINIMUM OF 2 WORKING DAYS FOR SETUP

(Acceptable Use Policy must be signed)

□ **New Access** □ **Change/Amend Access** □ **Remove Access** **User Name** □

EMPLOYEE DETAILS

First / Middle Name ____________ **Surname** ____________

Section ____________

Position ____________

Permanent Employee □ **Part Time / Temp** □

Part time/temps only. Network account will expire 1 month from start date if end date is left blank

Start Date ____________ **Expected End Date** ____________

If replacing a previous employee, please advise of -

Name of previous employee ____________ **Has this employee Resigned / Terminated?** □

OR Transferred to another Section? □

HARDWARE

This information is used to update the IT asset database.

Base Unit/Laptop Asset No ____________ **Other** *(please specify)* ____________

NETWORK ACCESS REQUIREMENTS

By default all new users will have access to Network, MS Office, MS Outlook, MS Internet Explorer

Some application & system access may have associated licence costs.

System / Application Name	Y	N	Same access as (enter a user name for EACH system/application)
Network ID (User Profile)	□	□	
Email	□	□	
Internet Access	□	□	
QL	□	□	
Astrow	□	□	
E:Drive	□	□	
S:Drive	□	□	
X:Drive	□	□	
Printer Access PIN	□	□	
iMail	□	□	
	□	□	

Supply Additional Information / Instruction of Access Requirements *(if necessary)* ____________

Please list email / security groups user to be included in:

Housing email. Security Groups,- All Staff, Domain Users, Housing and Tenancy Team.

Any Other Information □

AUTHORISATION *(Appropriate Manager)*

Name ____________ **Position** ____________

Signature ____________ **Date** ____________

APPLICATION FOR NETWORK ACCESS/REMOVAL

PLEASE ALLOW A MINIMUM OF 2 WORKING DAYS FOR SETUP

(Acceptable Use Policy must be signed)

□ **New Access** □ **Change/Amend Access** □ **Remove Access** **User Name** □

EMPLOYEE DETAILS

First / Middle Name ______________ **Surname** ______________

Section ______________

Position ______________

Permanent Employee □ **Part Time / Temp** □

Part time/temps only. Network account will expire 1 month from start date if end date is left blank

Start Date ______________ **Expected End Date** ______________

HARDWARE

This information is used to update the IT asset database.

Base Unit/Laptop Asset No ______________ **Other** *(please specify)* ______________

NETWORK REMOVAL REQUIREMENTS

Email forwarding will be removed after 30 days unless notified otherwise

System / Application Name	**Y**	**N**	**Please provide any additional notes as required**
Disable User	□	□	
Forward Email	□	□	Identify recipient if required
Back up E Drive	□	□	
Disable QL	□	□	
Back up My Documents	□	□	
Remove Printer Access	□	□	
Disable iMail	□	□	
Remove local PC profile	□	□	
	□	□	

Supply Additional Information / Instruction of Removal Requirements *(if necessary)* ______________

Please list email / security groups user to be removed from:

____

Any Other Information □

AUTHORISATION *(Appropriate Manager)*

Name ______________ **Position** ______________

Signature ______________ **Date** ______________