ICT Systems Security Procedure

Procedure Reference:		G15a	
Related Policy: Computer Systems, Email & Internet Policy		G15	
Effective date:	Sept 2021	**Review date:**	Sept 2024
Approved by P&PRG:		Sept 2021	
Owner:	Jean Stevenson	**Job Title:**	Head of ICT
To be issued to:		Board of Management All Staff	
Method of Delivery:		LearnPro / Induction	

Version Control

Date	Owner	Version	Reason for Change
Sept 2021	**Jean Stevenson**	**V 2.0**	**Rewritten in line with updated policy G15**

Summary of Changes

Section	Change
	This procedure replaces G46

ICT Systems Security Procedure (G15a)

Contents

1.0 Introduction

Ark has an obligation to its members to clearly define requirements for the use of its information and communications technology (ICT). This is to ensure that users of ICT facilities do not unintentionally place themselves, or Ark, at risk of prosecution, by carrying out computer related activities outside the law.

In addition, although the bulk of information held is intended to be openly accessible and available for sharing, certain information (key data and information) has to be processed, handled and managed securely and with accountability. Legislation is again the key driver of this requirement, but it is also derived from the criticality and sensitivity of certain information where loss of accuracy, completeness or availability could prevent Ark from functioning efficiently, or where disclosure could damage Ark's reputation or lead to legal proceedings.

1.1 Objective

Information Security controls are designed to protect all those associated with Ark and the Association's reputation through the preservation of:

- Confidentiality - knowing that key data and information can be accessed only by those authorised to do so;
- Integrity - knowing that key data and information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version; and,
- Availability - knowing that the key data and information can always be accessed.

Ark is committed to protect both, its staff and all authorised users, and its key data and information and to deploy controls that minimise the impact of any Security Incidents.

2.0 Applicability

The procedure applies to the following categories

- All staff, relief and agency staff employed by, or working for or on behalf of Ark;
- Contractors and consultants working for or on behalf of Ark;
- All other individuals and bodies, including Board Members, who have been granted access to Ark's ICT systems and/or key data and information.

Any breach of these procedures will be dealt with where necessary in terms of our disciplinary policy and procedures, or under the Board Members Code of Conduct, as appropriate. Serious breaches of these procedures will be considered gross misconduct in accordance with our disciplinary policy and procedures.

It is the personal responsibility of each person to whom the procedure applies to adhere with its requirements.

This procedure should be read in conjunction with the Computer System Security, Email & Internet Policy (G15), Openness & Confidentiality Policy (G13), Business Continuity Policy (G09), Data Protection Policy (G24) and related procedures.

3.0 Responsibilities

Through the Ark induction process all employees must signoff that they have read and understood the following prior to gaining access to Ark systems to reduce the risks of, theft, fraud or malicious misuse of facilities:

- Staff Code of Conduct;
- Computer System Security, Email & Internet Policy (G15);
- ICT Systems Security Procedure (G15a);
- Openness and Confidentiality Policy (G13).

Employee reference checking, Disclosure Scotland and Protection of Vulnerable Groups (PVG) checks are carried out prior to commencing employment in accordance with the Recruitment Policy, to minimise the likelihood of personnel, who pose a security risk, being employed in posts involving key data and information, such as those concerned with financial or personnel related data. All members of staff are bound by the Openness and Confidentiality Policy (G13) to protect confidential information in accordance with Ark's standard terms and conditions of employment.

Staff and all authorised users, are **not** permitted to:

- Disclose Ark email addresses to websites, unless there is a specific business reason for doing so;
- Join any mailing lists or solicit any information on the internet, unless there is a business need to do so;
- Use a home PC or device without authorisation from line manager/ICT which would include the end user's agreement on the minimum specifications of the devices including security/anti-virus levels. The devices must be maintained to the latest versions of the OS installed whether that be Microsoft or Apple. They must have approved anti-virus and a regular update of the anti-virus software. The Citrix Workspace should be updated when requested by ICT;

- Use Ark supplied devices for anything other than to conduct Ark business unless managers permission granted;
- Use devices issued for the use of Ark Information Management System (AIMS) for anything other than business use unless managers permission granted;
- Access to remote control software strictly regulated and used solely by ICT;
- Compromise the performance or privacy of any computer system;
- Place any comments and/or material on 'Social Networking' sites such as Facebook, YouTube, Twitter, Instagram, TikTok etc. that is critical, derogatory or defamatory about Ark or any of its Board Members, employees, tenants or supported people, or otherwise brings Ark into public disrepute, whether by using an Ark computer or a personal computer;
- Use WhatsApp or any other messaging apps or 'Social Networking' sites to share photographs or sensitive information on any Ark related matters including supported people unless they either have written approval from Ark manager or consent of the supported person or their welfare guardian.

Only designated staff will have the authority to add Ark material to Ark's website, publicly accessible websites, newsletters and social media profiles, unless specifically authorised to do so by the Chief Executive or the appropriate member of the Senior Leadership Team. All material will be checked for accuracy and the website, email newsletter and social media profiles will be updated regularly.

All staff will ensure that all online payments are made to secure websites only. This can be identified by both the padlock symbol on the address bar and the address of the website being prefixed by https.

Any member of staff, authorised individual or Board Member who knows or suspects that a colleague, Board Member or authorised individual is misusing the computer system or Ark hardware in any way should approach either their Manager, Director or the Chief Executive for a confidential discussion. If the concern relates to the Chief Executive, contact should be made with the Director of People & OD in the first instance.

The relevant manager will be responsible for ensuring that any temporary, freelance or consultancy staff has the required competence before they are allowed access to Ark's computer systems.

Visiting guests (e.g. freelance or consultancy staff, auditors etc.) requiring Wi-Fi access will be required to complete the Guest Wi-Fi use form (Appendix 1).

Board Members will be responsible for ensuring that any equipment that they use to access and/or process Ark or group company related data has to up to date virus protection software and password protection.

When a Board Member ceases their involvement with Ark, they will be required to delete or return all Ark or group company related data / equipment to the relevant department within Ark.

All Directors and Managers will be fully aware of the content of this procedure and ensure that it is followed by the staff they are responsible for.

All staff and Board members must ensure that they are familiar with the requirements of this procedure, and that they do not knowingly breach this procedure.

The relevant line manager is responsible for ensuring that each new employee receives a copy of this procedure and that Induction documentation is completed timeously.

The Head of ICT is responsible for advising the Leadership Team on all technical issues which may affect this procedure, so that they are dealt with promptly.

4.0 System Security Incidents

Events that are regarded as being 'security incidents' will be defined, and appropriate processes implemented to investigate, control, manage and review such events, with a view to preventing recurrence.

All system security incidents will be logged and maintained in the ICT helpdesk log. Each incident will be investigated and compared against the relevant system monitoring tools or logs depending on the nature of the incident. A full review will be undertaken to determine if there are any weaknesses in the security strategy and appropriate action deployed to prevent further incidents or patch identified flaws in software or procedures.

Those using or administering the ICT facilities must not try and prove any suspected or perceived security weakness. The exception to this rule is where ICT staff have been granted a specific policy exemption which allows them to do so as part of their role.

All actual and suspected security incidents are to be reported to the Head of ICT.

Any computer/system that is perceived to be placing the integrity of the network at risk will be disconnected at the network boundary. Subsequent reinstatement will only be permitted once the integrity of the system has been verified.

5.0 Remote Working

Whilst working remotely from Ark premises ICT reserve the right to remotely deploy critical system and software updates, anti-virus management and anti-virus software updates. Staff may also be requested to take mobile devices to Ark premises on an agreed date to be maintained.

These remote updates will be deployed every Friday, where required, (or the next online access thereafter) and as such will require system restart(s).

Ark employees must logout and shutdown laptops on a daily basis and allow any auto updates to run.

Non-critical but recommended software maintenance (for software such as Citrix Workspace and Microsoft Teams) to be undertaken routinely twice a year as part of an ongoing system health checks. Remote system health checks will be scheduled in advance and all users will be required to allocate time within their workload to accommodate this procedure.

Staff may also be requested to take laptops and chargers to Ark premises for Portable Appliance Testing (PAT).

6.0 Email

Ark employees may be given access to computers, email system, data and software. To ensure that all employees follow this policy, Ark may monitor computer and email usage. All Ark email is the property of Ark.

Board Members, staff and authorised individuals will not send or forward emails that contain inappropriate messages, including those that are:

- Sexually harassing or otherwise offensive to others on the grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation;
- Potentially defamatory, i.e. they criticise other individuals or organisations, or in any way disseminate unsubstantiated rumours about an individual or organisation;
- Being used as a medium for disciplining others, or for difficult or sensitive communication (criticising, advising, giving guidance) which is better done on a one to one, face to face basis;
- Appear to have been sent by someone else (even as a joke).

Board Members, staff and authorised individuals will not:

- Disclose anyone else’s email address without their express permission;
- Run or view messages or attachments from unknown senders, to minimise the risks from viruses or other malicious software;
- Forward confidential emails without the permission of the original sender;
- Email general confidential information or items of work related to supported people, tenants, customers or employees to or from personal email accounts.

Due to the insecure nature of the internet, email users should always consider whether the content of emails should be password protected. Highly confidential or valuable information will not be sent by email unless it is absolutely necessary to do so, in which case it will only be sent with the prior agreement of the relevant line manager, and be tagged as Confidential from the email system and sent with password protection.

All external emails sent will have the Ark email Disclaimer attached (Appendix 4).

7.0 Internet usage

Staff and authorised individuals may also access websites for personal reasons, but this must be done in their own time, e.g. during their lunch break and whilst in Ark property be subject to the conditions in the Acceptable Use Statement (AUS). Devices issued for the use of Ark Information Management System (AIMS) are solely for business use.

All users of the Ark Wi-Fi System must comply with this AUS.

> 'This AUS is intended to prevent unacceptable uses of the internet. Ark may remove, block, filter or restrict by any other means any materials that, in our sole discretion, may be illegal, may subject Ark to liability or may violate this AUS. Such accessing, downloading and/or circulation by authorised individuals will result in access to the Ark network being terminated, and will be reported by the relevant Ark manager to the individual's line manager either within Ark or in their own organisation. Ark may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong. Violation of this AUS may result in the suspension or termination of your access to the Wi-Fi System.'

Guests/visitors who require access to the Ark Wi-Fi will be required to complete the Guest Wi-Fi form (Appendix 1).

The use of personal ICT equipment (e.g. mobile phones, laptops, tablet devices) on the corporate network may be made available to staff, with Line Manager's permission, and will be liable to the same terms of the Acceptable Use Statement. Failure to adhere to the policy may result in these devices being denied further use of Ark's network. Anyone requiring such access should contact the ICT team after receiving approval from Line Manager.

Ark ICT reserve the right to monitor and control access to all Internet connectivity from all sites within Ark.

In making use of the internet and accessing websites, staff and authorised individuals will not access, view, receive, download, send or store material from websites or the internet that is:

- Sexual or pornographic (both adult and child pornography);
- Information on criminal activities or skills, including terrorism;
- Related to the activities of cults;
- Promoting gambling, or providing gambling opportunities on-line;

- Promoting or disseminating hate speech against individuals or specific groups;
- Promoting or encouraging violence against individuals or specific groups;
- Promoting or encouraging harassment, intolerance, racism or any other form of discrimination against individuals or specific groups;
- Promoting or selling illegal drugs;
- In any other way illegal;
- Known to be infected with a virus or other malicious material.

This list is illustrative, and not exhaustive. The accessing, downloading and/or circulation of such offensive material by Ark staff will be considered gross misconduct which will be dealt with in accordance with our disciplinary policy and procedures. Such accessing, downloading and/or circulation by authorised individuals will result in access to the Ark network being terminated, and will be reported by the relevant Ark manager to the individual's line manager in their own organisation. Hard copies or print outs will be provided to the individual's line manager as necessary.

This applies to the use of all Ark computer equipment, including that which is used / owned by supported people. Where supported people have their own equipment, staff and authorised users will be bound by this policy and will not support them in engaging in illegal activities.

8.0 Adding / removing staff and authorised individuals on the Ark network

8.1 All staff or Authorised individuals

To add all new staff (with the exception of Support Workers), non-Ark staff working for other group companies or someone contracted from another organisation ('authorised individual') who have been authorised to access the Ark network by the relevant Ark Manager or Director, to the system, the line manager or relevant Ark manager will complete a New ICT User Form (Appendix 2) and forward this by email to the ICT team at least 1 week before the employee/ authorised individual's start date. The ICT team will issue a 'user identity' (login ID) and the required password(s) to the line manager or relevant Ark manager.

The line manager/ relevant Ark manager will ensure that new staff or authorised individuals have read this procedure and signed the relevant induction documentation **before** they issue the user identity and password(s).

New Care & Support (Support Worker) staff will be issued with a password only, as they will be accessing existing accounts on the system. The line manager will ensure that new staff have read this policy and signed the relevant induction documentation before they receive their password.

For Staff/ authorised individuals ceasing employment or no longer requiring access to the Ark network the relevant line manager will complete an ICT User Leaving Form (Appendix 3). This will be passed (via the HR department for Ark Staff) to the ICT team prior to the effective leaving date. On or as soon as possible after their leaving date their account will be deactivated by ICT. ICT will delete the individual's details from the system one month from their leaving date unless the relevant manager makes a request to retain this data for a longer period of time.

When Care and Support (Support Workers) staff cease employment, or move to a different service, the manager must ensure that the password of the relevant account shared by service staff is changed.

8.2 User identity and passwords

Only the ICT team will have the authority to issue a 'new user identity' (login ID) and an initial password for a new account.

Following issue of their login ID and initial password, staff will be advised:

- To ensure that their initial password is changed ; staff will be automatically prompted to change their password at first login;
- All passwords are subject to a minimum complexity format and uniqueness state (same password cannot be re-used at a later date);
- That their password is confidential and must not be written down anywhere that could be accessible by others and should not be disclosed to any unauthorised person;
- Not to log into the network with any login ID or password other than the one issued to them, **except when** authorised to do so in advance for specific purposes by the relevant manager;
- If staff suspects that anyone else may know their password they should change their password immediately;
- Passwords should be created randomly to maximise security; passwords **should not** be created which form a pattern that ex-staff would be able figure out (e.g. month and year or service name with numbers after it);
- To maintain security, staff and other authorised individuals will be required by the system to change their login passwords every 42 days.

8.3 ICT Hardware and Software

All new ICT hardware and software (including mobile phones and removable storage devices) will be ordered by the ICT team in accordance with current procurement procedures, to ensure that the required standards are maintained and that the ICT asset register is kept up to date.

Ark employees should only use Ark issued hardware (including removable data storage devices such as USB memory sticks etc.) when conducting Ark business. The only exceptions to this will be as set out below.

Non Ark Issued hardware such as employees' own personal computers or laptops, will only be used in connection with Ark work with the prior approval of the relevant Line Manager and/or the Head of ICT. Such work will only be undertaken by employees through accessing Ark's secure Citrix infrastructure. Under no circumstances will Ark related work be saved by Ark staff onto hard drives, personal laptops/computers, or any other non-Ark supplied storage medium.

Members of the Ark Board of Management will be permitted to use their own personal computers, laptops, mobile phones or tablets in connection with Ark business, on the basis that Board Members will take responsibility for ensuring that Ark or group company data is secure at all times, password protected if necessary, and that such data is reviewed at regular intervals and deleted when no longer required. Board of Management Members wishing to dispose of hardware upon which Ark data has previously been saved should ensure that the hardware is securely disposed of, including full data wiping. Guidance can be sought from Ark's ICT team if required.

All software to be used on Ark's computers and laptops will be approved by the Head of ICT and licensed to the specified user. No software may be down loaded from the internet without the prior approval of the Head of ICT. Unauthorised copying of proprietary software is a breach of the Copyright Act and will be dealt with through Ark's Disciplinary Policy & Procedures.

All major software upgrades will be appropriately controlled and tested through a managed process before live implementation by authorised ICT staff.

8.4 Developing Applications

Staff and other authorised individuals who propose to develop small applications such as a database, spreadsheet or training application will ensure that they comply with this procedure, and in particular that they:

- Only develop such applications where there is a business reason for doing so;
- Comply at all times with the requirements of the UK General Data Protection Regulation;
- Do not expose themselves or Ark to adverse publicity, litigation or penalties by using software for which they have no licence to develop an application;

- Fully test any application before using it in a live environment;
- Put in place satisfactory security features to prevent misuse of the software and data;
- Develop adequate back-up procedures to protect the software and data.

8.5 Care and security of equipment, software and data

All staff and other authorised individuals will ensure that they take appropriate care of all hardware and software they use, including that of service users, to prevent loss or damage to the system and any applications and/or data held on it. The care and security measures will include:

- All hardware will be labelled by ICT with an identification number/serial number (labels **must not** be removed – if labels are worn/damaged please report to ICT);
- Hardware should not be tampered with (this includes mobile phones);
- Any Ark supplied equipment which is lost or stolen should be reported as soon as possible to the relevant line manager and ICT team;
- To prevent unauthorised access by others, staff must 'lock' their computer when leaving their workstation, and ensure they log out and switch off their computers when leaving work each day;
- Group policies are in place for Citrix access connections and user laptops to ensure that all devices / connections are locked after 15 minutes of inactivity;
- Those using Ark laptops will ensure that these are always left in a secure location and not unattended particularly when in public places (e.g. train stations etc.), and where possible that they are placed in lockable secure storage overnight;
- Every effort should be made to store any confidential/sensitive data on the Ark network. Where this is not possible an encrypted mobile device supplied by ICT team **must** be used;
- All removable data storage devices e.g., USB memory sticks etc. will be held in secure lockable storage;
- Removable data storage devices (USB Memory Sticks) will be supplied by ICT on request, and will be encrypted for security purposes;
- Any confidential, personal or sensitive information or data relating to supported people, tenants, employees or contractors, as set out in Ark's Openness and Confidentiality Policy and Data Protection Procedure will only be saved out with the Ark network removable storage with the prior agreement of the relevant member of the Leadership Team, Data Protection Officer and Ark's Head of ICT. In such cases, even if consent is obtained, such data will only be saved on ICT supplied encrypted removable storage devices;

- Where staff have the need to process Ark data on Ark issued laptops they should ensure that they back up the information at regular intervals onto a secure storage device (supplied by ICT), and that this is held separately in secure storage;
- Laptops will be subject to regular audit and maintenance by the ICT team.

8.6 Disposal of surplus hardware

Computer equipment that is no longer required will be identified by the Head of ICT, who will ensure that all data is deleted to ensure that no sensitive information is passed on to unauthorised persons.

Disposal will be carried out in accordance with the Disposal of Assets procedure ref: F22. Following disposal the Head of ICT will liaise with the Head of Finance/Finance Business Partner to update the asset register.

9.0 ICT Operations Management

9.1 Virus Protection

Anti-Virus technology is implemented to prevent the introduction and transmission of computer viruses both within and from outside the Association. This extends to managing and containing viruses should preventative measures fail. Real time monitoring identifies / alerts of any issues – should a potential threat arise this will either be automatically deleted, quarantined or blocked dependant on the nature of the threat that was identified by virus protection software.

9.2 Security Patches, Fixes and Workarounds

ICT is responsible for the day to day management of systems and to ensure that security patches, fixes and workarounds are applied in accordance with the agreed schedule. This is scheduled on a weekly basis and recorded in the Change Management Log with any issues identified being addressed and also documented in the Change Management Log. The Change Management log is a repository for all major system changes to be logged and documented. This log provides a history of change and the responsible personnel and is an invaluable tool in troubleshooting issues that occur and attempting to identify the source of the problem.

9.3 Vulnerability Testing

External Penetration Testing will be scheduled annually by ICT. Penetration Testing provides effective testing and reporting that details discovered vulnerabilities according to risk, provides descriptions of technical findings and provides mitigation advice for all identified vulnerabilities.

9.4 System, Application and Data Backup

All critical systems are managed in accordance with the following Backup procedure:

Once logged into the network, either on the physical network or via Citrix from the services, the files, emails and application data that are accessed are stored on network file servers. All files and all servers on the network located at the Priory are backed up every night of the week.

Ark uses a backup software product to perform daily system backups of all servers on the network and provide data retention and writes these backup images to a Network Attached Storage (NAS) device. This device acts as the primary storage device for backups. Depending on the nature of the server being backed up will determine the number of backup iterations that are stored on the backup NAS device. Servers that contain regularly changing data will have iterations that go back 6 months; servers that are mostly static in nature will have backup iterations of 3-4 weeks. These daily backups are copied to external drives (secondary storage devices) on a rota system to provide adequate cover for the server backups on the NAS. An external drive is attached to the NAS each weekday and removed the following day, the backup is set to run automatically each night, out with office hours. The backup copy is also set to run automatically every night to the external drives.

Each daily external drive is locked in secure storage, and the weekly drive is taken offsite every Monday and kept offsite till the following Monday. The scheduled quarterly drives are stored in the fire safe on the second floor and are replaced on an annual basis.

The backup software can be used to restore data and whole servers in case of accidental deletion, corruption or system failure. Item or system restores should be processed from the primary storage device.

Secondary storage drives provide additional cover to the data stored on the NAS device and can be used to restore data in the same manner as the primary storage device should the primary storage device be unavailable for any reason or for Disaster recovery.

Ark has a Business Continuity process that utilises this backup software to replicate the entire virtual server infrastructure every night of the week to an external partner as per the terms of the contract**.** In the event of a full Disaster Recovery event, the latest offsite external storage drive should be delivered to the external partner to provide extra resilience to the recovery procedure.

9.5 System Monitoring

System Monitoring encompasses management tools, manual scheduled processes and system alerts. These tools and scheduled processes augment and enable the daily proactive nature of the ICT department. Daily system checks for updates, patches, security vulnerabilities and industry wide recommendations, have to be verified, scheduled and implemented.

9.5.1 Management Tools

The Anti-Virus System Management console is responsible for much more than just the management of Anti-virus software. This facility reports the real-time status of:

- The virus condition of all Microsoft Windows devices on the network;
- The online status of all Windows Devices;
- The security status of all windows devices pertaining to patch levels;
- The security status of firewall settings for all Windows Devices;
- The health status with regards to disk space, memory and CPU resources of all Windows Devices.

The Hypervisor Management is responsible for management and configuration of all virtual servers:

- Installation/configuration and management of the VMware hosts;
- Installation/configuration and management of the VMware virtual servers;
- Patch management of all hardware and software components;
- Monitoring status of all CPU/memory/disc activity and Network statistics of all VMware virtual servers.

The Network Analyser is used to monitor the Network infrastructure of all HP switches:

- Real-time network monitoring of all interconnectivity and switch status;
- Patch management of all HP switches;
- Critical reporting of all major outages or network issues.

Backup & Replication Management console software manages our backup and replication processes:

- The results of every backup job for every server are reported and emailed to ICT;
- The results of every replication job for every server are reported and emailed to ICT.

Webfilter Portal is responsible for the monitoring and scanning of all Internet activity:

- All critical security issues such as malware are email to ICT;
- The "dashboard" feature display current and recent web activity highlighting risks and usage statistics;
- Reports on historical usage/top users/top sites/infected and blocked sites.

The External E-Mail Anti-Spam/Anti-Virus Portal is our management and configuration tool for all external Email in and out of the organisation:

- All critical security issues such as viruses are emailed to ICT;
- Real-time usage of all emails in and out of the system and their delivery status can be monitored;
- Allow and block list are configured;
- Reports on top senders/top receivers of email;
- Reports on viruses detected and whether quarantined or destroyed;
- SPAM reporting and configuration.

9.5.2 Manual Monitoring Processes

The weekly maintenance window utilises the planned downtime to:

- Patch all windows servers;
- Restart servers on a scheduled maintenance;
- Clear down user profiles[;
- Install/Upgrade software components
- Patch the Hypervisor environment;
- Patch the firmware levels of the firewalls, switches, webfilters and SANs.

9.5.3 System Alerts

All Hardware components configured to Email alert ICT of any critical change in status or outage. These devices include:

- The Hypervisor host servers;
- The Storage Area Network;
- The Webfilter Portal;
- The Core network switches;
- The Corporate Firewall;
- All the above mentioned System Monitoring tools.

10.0 Implementation and Review

10.1 Implementation

The Senior Leadership Team (SLT) is responsible for ensuring that this procedure is implemented throughout the organisation.

10.2 Review

The Head of ICT will ensure that these procedures are reviewed by the Policy & Procedure Review Group at least every 3 years.

Appendix 1 – Guest Wi-Fi User Form

Guest Wi-Fi Use Terms and Conditions Form

By obtaining Wi-Fi internet access utilizing Ark corporate network I agree to comply with the terms and conditions of Ark Acceptable Use Policy (AUP).

Acceptable Use Policy

All users of the Wi-Fi System must comply with this Acceptable Use Policy (AUP). This AUP is intended to prevent unacceptable uses of the internet. ARK does not actively monitor the use of the Wi-Fi System under normal circumstances. Similarly we do not exercise editorial control or review the content of any Web site, electronic mail transmission, newsgroup or other material created or accessible over or through the Wi-Fi System. However, we may remove, block, filter or restrict by any other means any materials that, in our sole discretion, may be illegal, may subject Ark to liability or may violate this AUP. Ark may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong. Violation of this AUP may result in the suspension or termination of your access to the Wi-Fi System.

On completion this form must be handed to ICT (by the relevant Ark manager) before you will be granted Wi-Fi access.

Signed: ____

Name: ____
[Please print]

Company: ____

Date: ______________________________

The above Acceptable Use Policy is a snapshot of the Ark staff terms and conditions of Internet Access Use – the complete relevant passage from this policy are available on request.

Appendix 2 – New ICT User Form

NEW ICT USER FORM

Upon completion of this form an account will be created for the named user enabling email and internet access as well as access to any systems or directories specified.

Line manager: Complete this form and email it to the ICT team **at least 1 week** before the date a new employee/ new authorised user starts/ requires access. Ensure that the Computer System Security policy and procedure have been given to the new employee/ user, and that they have read and understood them and signed the statement, **before** receiving their login ID and password(s).

NEW USER DETAILS				
Name:				
Location:				
Post title:				
Commencement date:				
End Date (If Temporary):				
Access required to: *(tick if required)*	Capita Housing		Capita Finance	
	HR/Payroll			
Directories:	Admin		Housing	
	Finance		New Finance	
	Personnel		Maintenance	
General Drive or Services Drive: *Please list folders for **full** access*				
Line Manager's name:		**Date:**		

For ICT use only

RECORD OF ACCOUNT OPENING			
Date account set up:		**User login ID:**	
Capita login ID (if required):			
HR/Payroll login ID (if required):			
ID & password passed to line manager on:			
Completed by:		**Date:**	

Appendix 3 – ICT User Leaving Form

ICT USER LEAVING FORM - ALL STAFF OR OTHER AUTHORISED INDIVIDUALS

All staff/ authorised individuals with access to ICT equipment who are terminating their employment with Ark/ no longer require access must complete this ICT User Leaving Form. Please complete the ‘User Details’ section then pass to the HR department who will forward it to the ICT team. In the case of a non Ark ICT user the completed form can be forwarded directly to the ICT team.

USER DETAILS	
Name	
Username	
Date of leaving Ark/ No longer requiring access	
Line Manager Name	
I have returned all software, data and ICT equipment belonging to Ark that has been issued to me and/or been in my possession.	
Date	
Employee/ Authorised individual’s signature	

For ICT use only

RECORD OF ACCOUNT CLOSURE			
Line Manager contact?		**Y/N**	
Specific user data requirements			
Capita account disabled			
Hardware log updated			
AD account and Exchange deleted			
Personal Directory and User Folders deleted			
Completed by:		**Date:**	

Appendix 4 – Email disclaimer

This message, together with any attachments, is sent subject to the following statements:

1. It is sent in confidence for the addressee only. It may contain legally privileged information. The contents are not to be disclosed to anyone other than the addressee. Unauthorised recipients are requested to preserve this confidentially and to advise the sender immediately.

2. It does not constitute a representation which is legally binding on the Association or which is capable of constituting a contract and may not be founded upon in any proceedings following hereon unless specifically indicated otherwise. This footnote also confirms that this email message has been swept for the presence of computer viruses.