ARK HOUSING ASSOCIATION LTD (ARK)

POLICY REF: G15
PROCEDURE REF: G46

Version 4.1 – August 2016

COMPUTER SYSTEM SECURITY, EMAIL & INTERNET POLICY

1.0 INTRODUCTION

1.1 This policy describes our arrangements for ensuring that:

- we use computer, e-mail and internet systems as effectively as possible;
- we have clear rules governing the use of computers, emails and the internet, and the security of the information held on our computer systems;
- all individuals who we authorise to use our systems are aware of these rules and the consequences of breaching them.

1.2 This policy covers the use of 'computer information systems' which includes:

- computers – office-based equipment and ARK laptops used out with the office and service users IT equipment;
- mobile phones;
- electronic mail (e-mail);
- the internet and World Wide Web browsers;
- all software applications used on computers;
- any other electronic media.

1.3 This policy is supported by detailed procedures, and should be read in conjunction with the Openness & Confidentiality policy G13, the Business Continuity policy G09 and related procedures.

1.4 Any breach of this policy and the procedure which supports it will be dealt with in terms of our disciplinary policy and procedures, or under the Board Members Code of Conduct, as appropriate. Serious breaches of this policy and the procedure which supports it will be considered gross misconduct in accordance with our disciplinary policy and procedures.

1.5 This policy has the following sections:

Section 2: ICT System Security Adding and removing staff/ other authorised individuals from the ARK network

- User identity and passwords
- ICT hardware and software
- Developing applications
- Care and security of equipment, software & data
- Confidentiality
- Disposal of surplus hardware

Section 3: Use of email

Section 4: Use of the internet & accessing websites

Section 5: Monitoring

Section 6: Implementation & review

1.6 This policy complies with the following legislation:

- Copyright, Designs & Patents Act 1988 (with regard to the copying of software)
- Malicious Communications Act 1988 (with regard to the sending of electronic communications)
- Misuse of Computers Act 1990
- Data Protection Act 1998 and related guidance
- Communications Act 2003 (section 127).

This policy also complies with Regulatory Standard 4 which states that:

'The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose.'

2.0 ICT SYSTEM SECURITY

Adding and removing staff/ other authorised individuals from the ARK network

a) All staff or other Authorised Individuals

2.1 To add all new staff (with the exception of Support Workers see 2.2.1), 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 1) and forward this by email to the ICT team 1 week before the employee/ authorised individual's start date. ICT team will issue a 'user identity' (login ID) and the required password(s) to the line manager or relevant ARK manager.

2.2 The line manager/ relevant ARK manager will ensure that new staff or authorised individuals have read this policy and the procedure which supports it, and signed the statement (Appendix 2) **before** they issue the user identity and password(s).

2.2.1 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 statement (Appendix 2) **before** they receive their password.

2.3 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 (i.e. the date when the staff member actually stops working at ARK, which may be before their last pay 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.

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

b) Temporary staff

2.4 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.

2.5 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 5).

2.6 For further details of the processes for adding and deleting staff to the system see the procedures supporting this policy.

c) Members of the Board

2.7 Members of the Board will be responsible for ensuring that any equipment that they use to access and/or process ARK or group company related data is subject to appropriate virus and password protection.

2.8 Members of the Board will be responsible for ensuring that they back up any information pertaining to ARK at regular intervals, onto a suitable secure storage device, the ICT team can advise if required.

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

User identity and passwords

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

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

- to ensure that their initial password is changed ; staff will be prompted to change their password at first login;
- 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.

2.12 To maintain security, staff and other authorised individuals will be required by the system to change their login passwords every 42 days.

ICT hardware and software

2.13 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.

2.14 ARK employees should only use ARK issued hardware (including removable data storage devices such as CDs, USB pens etc.) when conducting ARK business. The only exceptions to this will be as set out in section 2.15 below.

2.15 Non ARK Issued hardware such as employees' own personal computers, laptops, mobile phones or tablets 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 tablets, or any other non-ARK supplied storage medium.

2.16 Notwithstanding the above, 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.

2.17 Further guidance on storing ARK related work on ARK issued removable data storage devices such as CDs, USB pens etc. can be found at section 2.20.

2.18 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 a disciplinary offence.

Developing applications

2.19 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 policy and supporting procedures, 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 Data Protection Act;
- 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.

Care and security of equipment, software and data

2.20 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 will 'lock' their computer when leaving their workstation, and ensure they log out and switch off their computers when leaving work each day;
- 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 such as CD's, USB pens 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 service users, tenants, employees or contractors, as set out in ARK's Openness and Confidentiality Policy and Data Protection Procedure will only be saved outwith 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;
    - For Board Members please see sections 2.16 and 3.8.

2.21 The procedures supporting this policy give additional 'good practice' guidance on these and other care and security measures.

Confidentiality

2.22 All staff and other authorised individuals will ensure that they handle all the information they have access to in strict confidence, and that in particular they comply with the requirements of the Data Protection Act 1998, with our Openness & Confidentiality policy ref: G13 and our Data Protection procedures ref: G48.

Disposal of surplus hardware

2.23 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.

2.24 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.

3.0 USE OF EMAIL

3.1 All Board Members, staff and other authorised individuals will ensure that they comply with current legislation and good practice in their use of electronic mail (e-mail). Further guidance on double-checking intended recipients, using carbon copy and blind carbon copy, and sending emails to groups etc. can be found in the Procedure which supports this Policy.

3.2 In particular, when composing and sending emails Board Members, staff and authorised individuals will take into account those they:

- have the same status in law as other forms of written correspondence;
- may be used as evidence in any legal proceedings;
- may create a legally binding contract;
- may be accessed as part of an individual's request under the Data Protection Act for any personal or sensitive data we hold about them;
- may be accessed as part of a Freedom of Information Act request, insofar as this Act may apply to ARK's activities.

3.3 Emails sent from ARK network will have the current disclaimer attached (Appendix 4).

3.4 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; are potentially defamatory, i.e. they criticise other individuals or organisations, or in any way disseminate unsubstantiated rumours about an individual or organisation;

- are 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);
- are written in capital letters – considered to be the written equivalent of shouting;
- are 'global emails', i.e. to everyone in the organisation, except for official business purposes;
- are chain letters.

3.5 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 service users, customers or employees to or from personal email accounts.

3.6 Due to the insecure nature of the internet, email users should always consider whether the content of emails should be encrypted or 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 by an encrypted method or with password protection.

3.7 If an email is sent from a secure server to an insecure recipient, security will be threatened. Particular care should be taken when considering sending data to internet email accounts such as 'Gmail', 'Hotmail' or 'Yahoo mail'. Email users may need to check that the recipient's arrangements are secure enough before sending such messages, and if in doubt should check with ARK's Head of ICT before sending.

3.8 Whilst it is acknowledged that Board Members will sometimes require to email each other in relation to Board of Management business, they should ensure that email addresses are correct, should consider whether data requires to be sent by email at all, and if information is highly confidential or valuable should seek guidance from ARK's Head of ICT in relation to encrypting or password protecting relevant emails.

3.9 Email users will be permitted to make reasonable use of ARK's email facilities for personal matters. However should this facility be abused it may be withdrawn and the employee concerned may be subject to disciplinary action.

4.0 USE OF THE INTERNET & ACCESSING WEBSITES

4.1 ARK recognise that being able to access useful information on internet websites is a valuable benefit to staff in the carrying out of their duties. ARK also recognise however that internet access comes with a range of risks, and that those using the internet via the corporate network need clear rules and guidelines covering such access for their own benefit and that of the organisation.

4.2 Staff and authorised individuals will be permitted access to internet websites for business purposes. They will make reasonable use of this facility and will not spend excessive amounts of working time 'trawling' the internet for information. Staff and authorised individuals may also access websites for personal reasons, subject to the conditions in 4.3 below, but this will be done in their own time, e.g. during their lunch break.

4.3 All users of the Wi-Fi System must comply with this Acceptable Use Statement (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 5)

The use of personal ICT equipment (mobile phones, laptops, tablet devices, kindles etc.) on the corporate network can be made available to staff 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 ARKs network. Anyone requiring such access should contact the ICT team

4.4 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. Such activity may result in disciplinary action in terms of the relevant organisation's own policy and procedure. Hard copies or print outs will be provided to the individual's line manager as necessary.

4.5 Breaches of this policy as described above will be subject to disciplinary action. The decision as to whether the material listed above breaches this policy will be at the discretion of the Chief Executive, or a senior manager nominated by the Chief Executive.

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

4.6 Staff, authorised users, and where appropriate Board Members, will also not be 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;
- access an external computer or external network without specific prior authorisation from the Chief Executive or Head of ICT;
- compromise the performance or privacy of any computer system;
- place any ARK material on publicly accessible websites including the ARK website, unless specifically authorised to do so by the Chief Executive or the appropriate member of the Leadership Team;
- place any comments and/or material on 'social networking' sites such as Facebook, YouTube, Bebo, Twitter etc. that is critical, derogatory or defamatory about ARK or any of its Board Members, employees, tenants or service users, or otherwise brings ARK into public disrepute, whether by using an ARK computer or a personal computer.

Failure to adhere to the above conditions will result in action being taken under our disciplinary policy and procedures, or under the Board Members Code of Conduct, as appropriate.

4.7 All staff and authorised users will ensure that they do not infringe copyright law when downloading material for business purposes and/or forwarding it to others.

4.8 Where necessary, information received from the internet will be checked for reliability before being used for business purposes.

4.9 Only designated staff will have the authority to add material to ARK's website, email newsletter and social media profiles. All material will be checked for accuracy and the website, email newsletter and social media profiles will be updated regularly.

4.10 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.

5.0 MONITORING

5.1 ARK owns the information systems and has the right to audit and monitor them.

This means that email messages originating from, received into, or circulating within the ARK e-mail system remain the property of ARK regardless of their physical location.

5.2 It also means that ARK reserves the right to;

- inspect any and all files in private areas of the network in order to ensure compliance with this policy;
- remove any personal information held on the systems without notice.

5.3 The information held on ARK's computer systems, including details of all email traffic and of all access to internet websites, will therefore be monitored on a regular basis.

The Head of ICT, HR Director and Head of OD (Organisational Development) will have the authority to carry out monitoring checks on the use of the systems. The ICT team will monitor staff and authorised individuals access to internet sites and escalate any issues to the HR Director or Head of OD. The ICT team will monitor email traffic and all data saved on the system

5.4 Failure to comply with this policy will be a breach of ARK's rules and will result in the employee concerned being subject to disciplinary action, or the Board Member concerned being subject to action under the Board Code of Conduct. Hard copies of inappropriate messages or printouts of logs of internet access may be used as evidence in disciplinary proceedings.

Deliberate and/or significant breach of this policy may result in the dismissal of an employee or the Board Member concerned being subject to action under the Board Code of Conduct, and may also constitute a criminal offence.

Failure to comply with this policy, by authorised individuals who are not ARK employees, will potentially, 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. Such failure may result in disciplinary action in terms of the relevant organisation's own policy and procedure. Hard copies or print outs will be provided to the individual's line manager as necessary.

5.5 ARK has the right to make information it obtains from its monitoring processes available internally and/or externally including, where relevant, to such authorities as the Police.

Reporting misuse

5.6 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 in any way should approach their Director or the Chief Executive for a confidential discussion. If the concern relates to the Chief Executive, contact should be made with the HR Director in the first instance.

6.0 IMPLEMENTATION & REVIEW

6.1 The Chief Executive is responsible for ensuring that this policy and the supporting procedures are implemented throughout the organisation.

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

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

6.4 The HR Director is responsible for ensuring that each new employee receives a copy of this policy and the supporting procedure and the Statement for signature.

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

6.6 The Chief Executive will ensure that this policy is reviewed at least every 3 years.

Reviewed by the SLT: August 2016

Approved by the Board of Management: August 2016

Next review due by: August 2019

APPENDIX 1

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:				
Department / Location:				
Post title:				
Commencement date:				
Access required to: *(tick if required)*	Capita Housing		Capita Finance	
	HR/Payroll		Other	
Equipment required?	Thin Client		Laptop	
	Mobile Phone		Dongle	
	Other			
General Drive /Services Drive: *Please list specific folders required for **full** access*				
Line Manager's name:		**Date:**		

For ICT use only

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

APPENDIX 2

COMPUTER SYSTEM SECURITY, EMAIL & INTERNET POLICY AND PROCEDURE

I confirm that I have received a copy of the Computer System, Email & Internet policy and procedure, that I understand the policy and procedure, and that I agree to comply with the requirements of the policy and procedure:

Signed: _____

Name: _____
[Please print]

Date: _____

Following completion, this form should be passed to the HR department, to be added to the individual's personal file, or in the case of an individual who does not work for ARK, should be retained by the relevant ARK Manager.

APPENDIX 3

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	
Date	
I have returned all software, data and ICT equipment belonging to ARK Housing Association that has been issued to me and/or been in my possession.	
What Equipment was returned	**Who was it given to** -
Employee/ Authorised individual's signature	

For ICT use only

RECORD OF ACCOUNT CLOSURE **(this should be done 1 month after employees leaving date unless the relevant manager makes a request to retain this data for a longer period of time)**	
Line Manager contact?	**Y/N**
Specific user data requirements	
IBS account disabled	
AD account and Exchange deleted	
Remote mailbox, Profile directory & Personal directory deleted	
Completed by:	

APPENDIX 4

EMAILS - DISCLAIMER

This disclaimer will be attached to all external emails:

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.

Scottish Charity No: SC015694

APPENDIX 5

GUEST Wi-Fi USE FORM

By obtaining Wi-Fi internet access utilising ARK's corporate network I agree to comply with the terms and conditions of ARK's Acceptable Use Statement (AUS).

Acceptable Use Statement

All users of the Wi-Fi System must comply with this Acceptable Use Statement (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.

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 Statement is a snapshot of the ARK staff terms of Internet Access Use – the complete relevant passage from this policy is available on request.