ICT Acceptable Use Policy

Policy Reference Number: IT01

Effective date:	May 2025	**Review date:**	May 2028
P&PRG approval date:	April 2025	**Board approval date (Governance only):**	N/A
Owner:	Head of ICT Strategy & Development	**Department:**	ICT
To be issued to:	☒ Board of Management ☒ All Staff ☐ ET/LT ☐ Head Office Managers ☐ Department/other: ____________________	**Method of Delivery / learning to be shared**	☒ Annual Declaration ☒ Learn Pro Individual Sign Off ☒ Board Portal
Stakeholder Consultation	☐ All Staff ☐ Customer engagement ☐ Unite the Union ☐ Employee Voices Group ☐ EDIHR Group ☐ Department/other: ______________________	This policy will be reviewed every 3 years from the date of implementation or earlier if deemed appropriate for any legislation or regulatory changes. If this policy is not reviewed within the above timescale, the latest approved policy will continue to apply.	
Equality Impact Assessment		No	

Version Control

Date	Owner	Version	Reason for Change
Feb-25	Head of ICT Strategy & Development	1.0	Extraction of significant relevant sections from previous ICT policies into a new Acceptable Use policy specific to non-ICT users.

Summary of Changes

Section	Change
5	Extracted from G15 Computer System, Security, Email and Internet policy.
5.10	New section to reflect the emerging use of personal devices for work purposes.
5.17	New section to reflect the emerging use of AI tools.

Contents

1.0 Policy Statement

The purpose of this policy is to provide a safe framework for using Ark's Information and Communications Technology (ICT) infrastructure without exposing Ark to the risks which can come with its use.

This policy aims to:

- Ensure acceptable use of ICT by all users;
- Establish the parameters of appropriate use and best practice; and
- Protect Ark and users from potential legal liabilities.

Breaching this policy may result in disciplinary action, depending on the severity of the violation.

1.1 Legal & Regulatory Framework

This policy complies with the following legislation:

- Copyright, Designs & Patents Act 1988 (with regard to the copying of software);
- Investigatory Powers (Interception by Businesses for Monitoring and Record Keeping Purposes) Regulations 2018;
- Malicious Communications Act 1988 (with regard to the sending of electronic communications);
- Misuse of Computers Act 1990;
- Data Protection Act 2018;
- The General Data Protection Regulation (GDPR) and the UK General Data Protection Regulation (UK GDPR);
- Freedom of Information (Scotland) Act 2002;
- Communications Act 2003 (section 127).

This policy also complies with the Scottish Housing Regulator's 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 Scope

This ICT Acceptable Use Policy applies to all users who have authorised access and use of Ark ICT systems and services. Users include:

- Board of Management members;
- Ark employees, agency staff, volunteers or student placements; and
- Contractors or other external suppliers or stakeholders.

This policy covers the use of:

- All computers, laptops, and tablets;
- All telephone systems, including landline and mobile phones;
- All ICT systems and software, including email and internet access.

3.0 Roles & Responsibilities

There is a range of standard expectations which underpin all policies. Read more about Ark's standard roles and responsibilities. In addition, the following specific responsibilities apply to this policy.

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

4.0 Related Policies & Procedures or Relevant Documentation

New User and Leaver Forms can be found at Appendix 1 and 2 respectively.

- G24: Data Protection Policy

Ark's Vision, Mission & Values

5.0 ICT Acceptable Use

5.1 Overview

Use of ICT systems by users of Ark is permitted and encouraged where such use supports the goals and objectives of the organisation. However, users must ensure that usage complies with legislation and does not create unnecessary business risk to the organisation.

Users will only be authorised to access systems required for their specific job roles.

5.2 Agile Working

Ark will provide staff with the ICT equipment (excluding home internet connection) to work out-with an Ark office, where this is appropriate for their role.

ICT equipment includes, but is not restricted to, laptops, mobile phones, tablets, monitors, keyboard, and mouse. All ICT equipment will be owned and maintained by Ark.

Further information about agile working is included in the Agile Working Policy [HR13] and Procedure [HR13a].

5.3 New Users

To add new users who have been authorised to access Ark's ICT network by the relevant Ark Manager or Director, to the system, the relevant Ark manager (generally expected to be the users line manager) will complete a New ICT User Form (Appendix 1) and forward this by email to the ICT team.

Requests should be at least 1 week before the users start date. If a shorter notice period has been provided, Ark's ICT team cannot guarantee that new users will have the relevant devices, or access to Ark's ICT infrastructure, available to them from their first working day.

New users include:

- New Ark employees;
- New members of the Board of Management; or
- Non-Ark employees contracted from another organisation ('authorised individual').

The ICT team will issue a 'user identity' (login ID) and the required password(s) to the line manager or relevant Ark manager.

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

Where access to Citrix is limited to a shared user log-in. New users will be issued with a password only, as they will be accessing existing accounts on the system. Managers will ensure that new staff have read this policy and signed the relevant induction documentation before they receive their password.

5.4 Removal of Users

For employees ceasing employment and authorised individuals no longer requiring access to the Ark network, the relevant manager will complete an ICT User Leaving Form (Appendix 2).

This form should be passed (via the HR department for Ark Staff) to the ICT team prior to the effective leaving date (or as soon as practically possible).

On or as soon as possible after their leaving date the user 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.

5.5 Unacceptable Behaviour

The following is deemed unacceptable use or behaviour by Users:

- Viewing, downloading, creating, or distributing any inappropriate content;
- Viewing, downloading, creating, or distributing any Ark information through a system that is not an authorised ICT system. This may include a personal email account, instant messaging systems such as whatsapp, photographs on personal devices, an unsanctioned cloud storage service, open-AI systems, or connecting personal storage devices to the organisation network;
- Using any ICT system for any illegal or criminal activities including any form of fraud, hacking/use of malware, piracy;
- Violating Copyright and Intellectual Property Rights legislation;
- Using any ICT system to create, or distribute unsolicited “nuisance” emails, or material which is used to facilitate harassment, bullying and/or victimisation of another member of staff or a third party;
- Disclose Ark email addresses to websites, unless there is a specific business reason for doing so;

- Viewing, downloading, creating, or distributing material that brings Ark into disrepute;
- Intentionally or recklessly introduce any form of spyware, computer virus, or other potentially malicious software; or
- “Jailbreaking” or “rooting” any Ark device.

This list is illustrative, and not exhaustive.

5.6 Security

All actual and suspected security incidents are to be reported to the Head of ICT Strategy Development, who will implement appropriate processes to investigate, control, manage and review such incidents, with a view to preventing recurrence.

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.

Those using or administering 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.

Users must not leave any device logged on in their name and unattended. When away from the device, staff should lock the device screen to prevent unauthorised access.

Where multiple users share PCs/terminals (such as a shared office computer or meeting room PC used for video calls), users must protect the confidentiality of messages and information sent to them. To protect this information, employees must log-off when they have finished using a shared PC.

Under no circumstances will Ark related work, including photographs, be saved by Ark staff onto non-Ark supplied hard drives, desktops, laptops, mobile phones, or any other storage medium.

5.7 Passwords (Password Complexity)

All users will be issued with a unique Username and initial Password to be used to connect to Ark’s network.

Users will be required to change the password twice a year. Passwords should not be written down, kept where others might find them, or shared with anyone else.

When creating a new a password, users will need to follow the password complexity rules, these are:

Password must be at least 12 characters long and contain at least one of each of the following.

One capital letter	e.g. A
One number	e.g. 1
One special character	e.g.!

A user's account will be locked out after 10 failed attempts in a row.

5.8 Multi-Factor Authentication

Multi-Factor Authentication ("MFA") is increasingly being used to strengthen user identity checks before allowing access to ICT services and systems.

Where allowed, MFA will be used as standard across Ark's software and systems.

5.9 Hardware – Provided by Ark

ICT hardware provided to users is the property of Ark. Users are accountable for the use of the ICT device provided to them by Ark and should not lend devices to anyone or otherwise permit use by anyone else.

Devices are identified by an asset tag and unique asset number. This identification should never be removed from the device.

Adequate safeguards must be taken to protect all equipment allocated to users by Ark. When not in use, users should always store devices somewhere safe, where it cannot be easily seen from outside and out of reach of children and pets. Devices should never be left in a vehicle overnight.

Ark employees must logout and shutdown laptops daily and allow any software auto-updates to run.

Should hardware be damaged, lost, or stolen in your care, you must report this to your manager and ICT immediately.

Ark cannot recover information stored on personal or corporate devices if the device is lost, damaged, or stolen. Ark data and information must be stored in a networked location provided for that purpose (Citrix or SharePoint).

Ark owned devices must not be removed from the UK. In exceptional cases, exceptions can be granted for Agile Workers and must be approved by a member of the Executive Team, after liaising with ICT and Compliance & Improvement departments.

Upon ceasing to be a user of ICT systems, hardware must be returned to ICT (via your manager), to allow for it to be re-used.

If static computer equipment (such as PC's, Thin clients, printers and networking equipment) requires to be relocated (for example, as part of an office move), the relevant manager should liaise with the ICT department, who are responsible for maintenance and relocation.

5.10 Hardware – Bring Your Own Device ("BYOD")

All Ark employees and members of the Board of Management may, where their preference is to do so, use their own devices when conducting Ark business.

Ark Employees

We recognise that staff may prefer to use their own mobile phone, particularly front-line Support Workers when recording AIMS activity, rather than carrying an Ark tablet or a second mobile phone device.

Staff that have an Ark email address may download the Microsoft Intune app (Company Portal) to their personal phone, which will give them access to the business applications that they require.

Staff must use the secure links provided by Ark to process data when using their own personal device. Ark data should not be stored on personal devices at any time.

Further guidance for employees can be found in the 'Bring Your Own Device' [IT01a] procedure.

Board of Management

Ark’s Board of Management access Ark documentation via their Microsoft 365 account. Board Members are responsible for ensuring that Ark data is not downloaded onto personal devices.

5.11 Software

Where software is required to be installed on Ark devices or managed by the ICT department (such as Microsoft 365), the ICT department will provide users with access to the software they require to perform their role.

Commercially licenced software remains the property of Ark and may not be copied from Ark systems by any users for any purpose.

Only ICT Administrators, which include Ark’s external ICT consultants, are permitted to install software, including patches or updates which may change the functionality of that software.

Users may not install any software or applications onto devices. If there is a defined business need for additional software, initial approval should be sought from the users’ manager before liaising with ICT via the Service Desk.

Software is increasingly being provided as a service via the Cloud, accessed via a web browser. This includes Ark’s Care & Support, Housing Management, and Finance systems. User access to these systems will be managed by the appropriate business owners.

5.12 Telephones and Mobile Phones

Users are expected to use phones for the duties that they are required to undertaken.

ICT can track telephone calls (number called/duration of call/mobile data usage). Users must not call international or premium rate numbers or knowingly participate in telephone fraud.

Mobile phone data usage should be used only for the delivery of business activity. High individual levels of mobile data usage will be investigated and where necessary, alternative arrangements will be put in place (additional data plan, Wi-Fi, training).

5.13 Emails

All attachments received from third parties must be treated with caution. Incoming emails are where most security threats arise. Although all incoming emails are checked for embedded viruses, this cannot stop all emails of a malicious nature.

Users must remain vigilant when opening emails and attachments, attachments should not be opened from an unsolicited source. If users are in doubt as to its content, clarification should be sought from ICT.

Users should not use their Ark email address when signing-up for non-business-related services. These email addresses can and will be passed onto other organisations and will increase the level of spam coming into the organisation.

Ark may monitor computer and email usage, and all Ark email is the property of Ark.

When composing and sending emails, users will consider that emails:

- 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; and
- May be accessed as part of a Freedom of Information Act request, insofar as this Act may apply to Ark's activities.

In line with Ark's Record Management policy [G25], emails will be automatically deleted 12-months from date of receipt, unless saved down onto the network or software database.

5.14 Internet and Wi-Fi Use

The Internet is largely unregulated; therefore, care should be taken when accessing information from it, or when browsing unfamiliar websites. Compromised websites may be used to trick users into accidentally activating malware.

All users are granted access to the Internet. The Internet may be used to seek information on matters relevant to the user's role.

All users of the Ark Wi-Fi System must comply with the following 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 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.'

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.

5.15 Personal Internet Use

Ark recognises that the Internet is embedded in many people's daily lives. As such, users are allowed to use the Internet for personal reasons, providing that personal use should be of a reasonable level and restricted to non-work times, such as breaks and during lunch.

All rules described in this policy apply equally to personal internet use. For instance, inappropriate content is always inappropriate, no matter whether it is being accessed for business or personal reasons.

5.16 Social Networks

Information posted on Social Networks is classed as public, and therefore potentially available for anyone to view.

Users should not disclose confidential information relating to Ark or its stakeholders, on any social networking site. Users should also not post any comments on people or events connected to Ark or make any remarks which could potentially bring Ark into disrepute. Any such actions could result in disciplinary action, including dismissal.

5.17 Use of Artificial Intelligence (AI)

As the use of Artificial Intelligence (AI) technologies evolves, it is important for users to understand how they may be applied within Ark's ICT infrastructure. AI tools and services may be integrated into certain processes to enhance productivity, decision-making, and operational efficiencies with department approval.

Users must ensure that any use of AI tools complies with Ark's data protection, security policies, and all applicable legal and regulatory frameworks. AI should only be used for business purposes that support Ark's objectives and must not be used to perform tasks that would ordinarily require human judgment or intervention, unless explicitly authorised by Ark's Senior Leadership Team.

Any AI tools used with Ark's information must be closed systems that do not retain, learn from, or share data externally.

Employees must not upload or share any data that is personal, confidential, proprietary, or protected by regulation within the AI system. This includes data related to customers, clients, employees, or other third parties, and in particular, information that:

- can identify any of the above-mentioned individuals;
- is considered sensitive in its nature; or
- is personal or special category personal data as defined under Articles 4 and 9 of UK GDPR.

Employees must be mindful of whether it is possible to indirectly identify an individual from the content entered into an AI system, i.e. asking AI to write a Job description which relates to a position held by only one person. If you intend to process personal data using an AI product, then it is recommended that you carry out a DPIA.

It is the responsibility of users to ensure that AI-generated data or outputs are reviewed by a qualified individual to ensure accuracy and appropriateness before being shared or acted upon. Users should be mindful that AI systems may contain biases and should not rely on AI alone when making decisions that affect individuals or sensitive information.

Employees should recognise the limitations of AI and always use their judgement when interpreting and acting on AI-generated recommendations. AI systems should be used as a tool to augment human decision-making, not to replace it.

Any use of AI technology outside of the approved, operational use cases must be reported to the Head of ICT Strategy & Development, and/or the Head of Compliance department for review.

6.0 Ark's Training & Monitoring Requirements

6.1 Training

All staff will have training appropriate to their needs and to the needs of the organisation as identified on their individual learning plans. Ark will ensure that relevant employees have an awareness of this policy and receive adequate training to enable them to effectively fulfil their roles and ensure Ark's ICT infrastructure remains safe and resilient.

6.2 Cybersecurity Training

All Ark employees will complete annual Cybersecurity training.

The cybersecurity training is intended to reinforce positive behaviours and ensure users understand the risk and vulnerabilities created by ignoring the rules outlined in this document.

Cyber resilience and lessons about good cyber hygiene will be communicated periodically throughout the year by the ICT department, aligned to current trends and threats.

If you do not understand the implications of this policy, how it applies to you, or would like to seek additional ICT training, please contact the ICT Service Desk for advice.

6.2 Monitoring

ICT systems are provided for legitimate business use. The organisation therefore reserves the right to monitor or examine systems and review the information stored or transmitted through those systems to ensure compliance with this policy.

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.

Appendix 1: 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)*	Rubixx Housing		Rubixx Accounts	
	HR/Payroll		AIMS	
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:**	
Rubixx login ID (if required):			
HR/Payroll login ID (if required):			
ID & password passed to line manager on:			
Completed by:		**Date:**	

Appendix 2: 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			
Rubixx account disabled			
Hardware log updated			
AD account and Exchange deleted			
Personal Directory and User Folders deleted			
Completed by:		**Date:**	