ICT Security Policy

Policy Reference Number: IT02

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: ____ICT_____	**Method of Delivery / learning to be shared**	☒ Annual Declaration ☐ LearnPro 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
May-21	Head of ICT Strategy & Development	5.0	New policy format / cyclical review
Feb-25	Head of ICT Strategy & Development	6.0	Cyclical review

Summary of Changes

Section	Change
Policy Name	Policy reference and name changed from "G15 Computer System Security Email Internet policy" to "IT02 ICT Security Policy". Policy now to be issued to ICT staff and contractors only, with a new IT01 Acceptable Use Policy introduced for non-ICT staff.

Contents

1.0 Policy Statement

The use of Ark's Information and Communications Technology (ICT) hardware and software is fundamental to enabling the delivery of Ark services to customers and stakeholders.

This policy sets out clearly defined processes to ensure the protection of confidentiality, integrity and availability of Ark information and ICT infrastructure.

It does this by providing a safe framework for protecting Ark's ICT infrastructure (hardware and software), which holds key data and information to allow for the smooth running of the organisation.

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).

2.0 Scope

This ICT Security Policy applies to all ICT staff and external ICT consultants who have authorised 'super-user' access and use of Ark ICT systems and services.

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 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 procedure applies to adhere with its requirements.

4.0 Related Policies & Procedures or Relevant Documentation

This policy should be read in conjunction with the following procedures:

- ICT01: ICT Acceptable Use Policy
- IT02a: ICT Security Procedure
- IT02b: ICT Systems Monitoring and Patching Procedure

Ark's Vision, Mission & Values

5.0 ICT Security

5.1 Overview

Computer systems and networks in Ark are protected by suitable physical, technical, procedural and security controls.

Controls will be implemented as appropriate to prevent unauthorised access to, interference with, or damage to, Ark's ICT infrastructure and data.

5.2 Organisational Security

Access to Ark information processing facilities by third parties is controlled by ICT. Information assets (hardware & software) are categorised and recorded to enable appropriate management and control. Inventories of information assets, including hardware, software and key data are developed and maintained by ICT.

Ark use third party software for company functions which are cloud based and not managed by the Ark ICT department, the software/applications are manged by the department who use them.

5.3 New Users

Only the ICT team will have the authority to issue & manage ‘core’ system access. This includes Citrix, Microsoft 365, and any other software directly located on Ark devices (such as servers or laptops).

For specific cloud-based business applications where access is via a web browser, such as Ark’s Care, Housing and Finance systems, access is maintained by relevant departmental business owners.

5.4 Changes to User Access

Any change required for a user will be made by the user's line manager via an email request sent to the ICT helpdesk. It should clearly state what change is required. ICT will then confirm to the manager and user when the change has been enacted.

5.5 Removal of Users

The ICT Helpdesk must be notified in a timely manner of any member of staff leaving or who no longer require access to Ark ICT systems, using the leavers form. All users access will be disabled on processing the leavers form and their account will then be deleted after one-month.

Any manager requiring access to the leavers data or would like to retain the account for longer should state this in the leavers form.

5.6 Physical and Environmental Security (Including Server Room and Office ICT Equipment)

Controls will be implemented as appropriate to prevent unauthorised access to, interference with, or damage to, ICT assets.

Computer systems and networks are protected by suitable physical, technical, procedural and security controls.

Access to all core, networking and Server Room equipment in the infrastructure are situated in physical secured areas - either in a secure room and/or secure cabinets. Access to these areas is restricted to ICT and permission to access these areas out-with ICT staff must be obtained from the Head of ICT Strategy & Development.

The Server Room has further environmental security features that reflect the critical nature of the equipment and data held within this area. This room is temperature controlled by air conditioning, which is regularly maintained by an external supplier. All server, storage and networking equipment are installed with redundancy or failover equipment to ensure system resilience. All server, storage and networking equipment are further protected by a dual Uninterrupted Power Supply (UPS) system to ensure uptime and failover in the event of an electrical outage.

All static computer equipment is controlled by the ICT department. This includes PCs, Thin clients, printers and networking equipment.

This equipment will be maintained and updated by ICT staff. ICT staff are responsible for the siting and location of all computer equipment. Relocation of this equipment must be carried out by ICT personnel or at least with their approval after appropriate consultation.

5.7 Responding to Security Incidents

Events that are regarded as being 'security incidents' will be recorded in the Change Management Log, and processes implemented to investigate, control, manage and review such events, with a view to preventing recurrence.

Security incidents can include:

- Disclosure of passwords;
- Un-authorised access to applications or data;
- Receiving of malicious emails, and/or responding to malicious/phishing emails;
- Malicious attack carried out be member of staff with access to systems.

5.8 ICT Hardware

All new ICT hardware (including laptops, mobile phones, tablets, monitors, docks and peripherals) will be ordered by the ICT team in accordance with Ark's Procurement Policy [F02] to ensure that the required hardware standards are maintained, and that the ICT asset register is kept up to date.

Members of staff can request different hardware if there is a business case or requirement. Staff also can request hardware to help support Agile working.

5.9 Software Updates

Software updates should be applied as soon as practically possible, to minimise the security risk.

Non-critical but recommended software maintenance (for hardware and software such as HP and Microsoft) will be carried out by ICT where applicable.

ICT will monitor updates and prompt users to update software where necessary.

5.10 Mobile Device Management

Microsoft Intune will be used for management and securing of Ark owned devices using Mobile Device Management ("MDM"). This software will be installed on all Ark laptops, tablets, and mobile phones before they are rolled out to users.

MDM is used to manage, monitor, track and secure devices and enables centralised control.

For mobile phones and tablets, MDM will also enforce a PIN code to be set, adding an extra layer of security. Ark reserves the right to remotely wipe the devices should they be reported lost or stolen.

5.11 Emails

All emails originating from outside the company will have yellow banner stating the email is from an external source.

The ICT Helpdesk should be made aware of any malicious or nuisance emails (a suspicious email may be from a known recipient but asking for something out with the norm). These should be added to the filter and will no longer be received by anyone in Ark.

All external emails sent will have an Ark email Disclaimer attached (Appendix 1).

5.12 Internet and Accessing Websites

ICT will restrict access to known malicious and unsuitable sites. Restrictions are also in place to prevent users accessing any links/sites promoted or displayed for advertising purposes.

6.0 Ark's Training & Monitoring Requirements

6.1 Training

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 Monitoring

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 email system remain the property of Ark regardless of their physical location.

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; and
- Remove any personal information held on the system without notice.

The information held on Ark's computer systems, including details of all email traffic and access to websites, will therefore be monitored on a regular basis by the ICT department. Issues will be escalated to the Leadership and/or Executive Team.

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

Appendix 1: 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.