Computer System Security Email Internet Policy

Policy Reference:		Insert policy reference G15	
Effective date:	April 2021	**Review date:**	April 2024
Approved by SLT:	April 2021	**Approved by BoM:**	May 2021
Owner:	Jean Stevenson	**Job Title:**	Head of ICT
To be issued to:		Board of Management ARK Management All Staff	
Method of Delivery:		LearnPro	

Version Control

Date	Owner	Version	Reason for Change
Mon 2021	**Jean Stevenson**	**V 5.0**	**New policy format / cyclical review**

Summary of Changes

Section	Change
	New template applied / general updates

Computer System Security Email Internet Policy

Contents

1.0 Ark Values 3
2.0 Purpose 3
3.0 Policy Statement 4
4.0 Scope 4
5.0 Legal/Regulatory Framework 4
6.0 Responsibilities 4
6.1 Board of Management 5
6.2 Executive Team 5
6.3 Senior Leadership Team 5
6.4 Managers 5
6.5 All Staff 5
6.6 Non Ark employees 5
7.0 Computer System Security, Email & Internet Usage 5
8.0 Related Policies & Procedures 9
9.0 Equality Impact Assessment (EIA) 10
10.0 Data Protection Impact Assessment (DPIA) 10
11.0 Stakeholder Consultation 10
12.0 Monitoring and Review 10
12.1 Monitoring 10
12.2 Review 10

1.0 Ark Values

Ark values are true to the core purpose of the organisation and the services we deliver. They determine our behaviours towards one another and what we should expect in our relationships with one another. Working within the following values will guide and help us deliver our vision and mission of Ark being an organisation where everyone is equal:

Trust

We have confidence in our people to deliver excellent services and trust in them to do so. We will develop trusting and honest relationships and our customers will feel assured that they can rely on us to deliver.

Respect

We treat everyone fairly and we listen. We are respectful of each person with whom we come into contact and expect our people to respond professionally and treat others as they would wish to be treated.

Understanding

We will operate with empathy and compassion and approach each situation with an open mind. We will question and challenge to ensure we achieve the right outcomes for customers and our people.

Equality

We believe everyone is equal and expect our people to create positive experiences where everyone feels valued and included.

Integrity

We will do the right thing and take responsibility for our actions. We will work together to uphold the highest standards of behaviour and practice.

2.0 Purpose

The purpose of this policy, and supporting procedures is to provide a framework for protecting Ark's ICT infrastructure, key data and information to ensure that these services, including email and internet usage, are used responsibly in line with good practice and legislation.

3.0 Policy Statement

This policy sets out to ensure that Ark has a clearly defined process in order to ensure:

- The protection of confidentiality, integrity and availability of Ark information and infrastructure.
- All users are aware of and comply fully with all relevant legislation.
- All staff understand the need for information and ICT security and their own responsibilities in this respect.

4.0 Scope

All Board of Management members, all staff, relief, agency, contractors who access Ark's ICT systems are required to abide by this policy.

5.0 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 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.'

6.0 Responsibilities

6.1 Board of Management

Ark's Board of Management is responsible for consideration and approval of this policy, and for ensuring that its decisions are taken in accordance with relevant regulatory expectations, good practice, training and guidance.

6.2 Executive Team

Ark's Executive Team is responsible for ensuring that this policy is reviewed in accordance with Ark's schedule for review of policies, or sooner if required. The Executive Team is responsible for ensuring that its decisions, and the decisions of officers, are taken in accordance with relevant regulatory expectations, best practice, training and guidance.

6.3 Senior Leadership Team

The Senior Leadership Team will be responsible for approval of this policy and the effective implementation of this policy within their area of responsibility, as required. They must also ensure that each member of their staff, through induction, and team meetings, is made aware of this policy and participates in relevant training.

6.4 Managers

Ark Managers will be responsible for the effective implementation of this policy within their area of responsibility, as required. They must also ensure that each member of their staff, through induction, and team meetings, is made aware of this policy, local plans and participates in relevant training.

6.5 All Staff

All Ark employees are required to familiarise themselves with this policy and comply with its provisions as well as undertake any training implemented as part of the rollout of this policy.

6.6 Non Ark employees

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.

7.0 Computer System Security, Email & Internet Usage

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 information assets.

7.1 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. Detailed description of responsibilities and guidelines are in the supporting procedure (G15a). Key data and information will be classified and managed in accordance with the General Data Protection Regulation (GDPR).

Only the ICT team will have the authority to issue & manage system access including all login ID's at Ark. For specific business applications there are super users assigned to maintain application access. All ICT hardware and mobile devices are issued by ICT and staff should not amend or remove any configuration settings.

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.

7.2 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, *information 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 all of these areas is restricted to ICT and permission to access these areas out with ICT staff must be obtained from the Head of ICT.

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 ARK ICT. 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.

7.3 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.

7.4 ICT Hardware & Software

All new ICT hardware and software (including mobile phones, tablets and removable storage devices) will be ordered by the ICT team in accordance with current procurement procedure (F02a), to ensure that the required standards are maintained and that the ICT asset register is kept up to date.

Ark employees should use Ark issued hardware (including removable data storage devices such as USB memory sticks etc.) when conducting Ark business.

Non Ark issued hardware such as employees' own personal computers, tablets, mobile phones or laptops, will only be used in connection with Ark work with the prior approval of the relevant Manager and/or the Head of ICT. Such work will only be undertaken by employees through accessing Ark's secure Citrix infrastructure ensuring all documents saved in Citrix or any Ark approved Ark applications e.g. Ark Information Management System (AIMS) – Access Care Planning.

Under no circumstances will Ark related work be saved by Ark staff onto hard drives, desktops, 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.

7.5 Remote Working

Ark will provide staff with the ICT equipment (excluding home internet connection) to work out with an Ark owned or leased building, where this is appropriate for their role. ICT equipment includes, but is not restricted to, laptop computers, mobile phones, desktop thin clients, tablets, monitors, keyboard, and mouse. All ICT equipment will be maintained by Ark.

Ark employees must not change any configuration or settings within Ark devices without written consent.

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

When working in Ark premises or remotely, staff must not allow access to Ark equipment by any unauthorised individuals.

Further details of remote working should be read in the supporting Agile Working Policy (HR13) and Procedure (HR13a), and ICT Systems Security Procedure (G15a).

7.6 Mobile Phones

Mobile Device Management (MDM) software will be installed on all Ark mobile phones. MDM is used to manage, monitor, track and secure mobile phones and enables centralised control of Ark mobile phones. MDM also enforces a PIN code to be set for all phones adding an extra layer of security. Ark reserves the right to remotely wipe the phones should they be reported lost or stolen. Ark employees who have an Ark mobile phone should not change configuration settings.

7.7 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 and all Ark email is the property of Ark.

When composing and sending emails Board Members, staff and authorised individuals will take into account that these 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;
- May be accessed as part of a Freedom of Information Act request, insofar as this Act may apply to Ark's activities.

Our aim is to have a workplace that is free of harassment and sensitive to the diversity of our employees. Therefore, we do not allow employees to use computers and email in ways that are disruptive, offensive to others, or harmful to morale.

Emails sent from the Ark network will have the current disclaimer attached.
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.

7.8 Internet & Accessing Websites

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.

Staff and authorised individuals will be permitted access to internet websites for business purposes. Online streaming should be discouraged/prohibited unless for specific business use.

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.

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

7.9 System Review 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 e-mail 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;
- Remove any personal information held on the systems without notice.

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

8.0 Related Policies & Procedures

This policy should be read in conjunction with Ark's:

- ICT Systems Security Procedure G15a;

- ICT Systems Monitoring & Patching Procedure G15b
- Business Continuity Procedure G44;
- Business Continuity Plans;
- Business Continuity Actions Plan – Director of People & OD;
- Recruitment Policy & Procedure HR01;
- Agile Working Policy and Procedure HR13, HR13a

9.0 Equality Impact Assessment (EIA)

No potential equalities issues have been identified in relation to the development of this policy, and consequently an EIA has not been completed.

10.0 Data Protection Impact Assessment (DPIA)

Please see ICT Data Protection Impact Assessment.

11.0 Stakeholder Consultation

In developing this policy the following groups were consulted:

- Ark Board of Management;
- Ark Executive Team; and
- Ark Senior Leadership Team.

12.0 Monitoring and Review

12.1 Monitoring

Ark's Executive and Senior Leadership Teams will monitor implementation of this policy on an ongoing basis.

12.2 Review

This policy will be reviewed within 3 years from the date of approval by our Board of Management, in accordance with Ark's policy review framework.