IT ACCEPTABLE USE FOR STAFF POLICY

Date of last review:	April 2012	**Review period:**	2 years
Date of next review:	April 2014	**Owner:**	IT Director
Type of policy:	Network	**LGB or Board approval:**	Board

ARK IT ACCEPTABLE USE POLICY

1.0 Overview

1.1 The intention in publishing and deploying an Acceptable Use Policy is not to impose restrictions that are contrary to the established culture of openness, trust and integrity. ARK is committed to protecting employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.2 All information technology assets procured or funded by ARK IT including but not limited to computer equipment, software, operating systems, storage media, network accounts providing email, WWW browsing, and SSL Explorer are the property of ARK and are governed by this policy. These systems are to be used for business purposes in serving the interests of the organisation.

1.3 Section 8 "Professional Responsibilities" covers all users using information technology assets in any capacity whether they are procured or funded by ARK or part of the user's domestic or personal provision.

1.4 Acceptable and appropriate use is a team effort involving the participation and support of every ARK member of staff. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

2.1 The purpose of this policy is to outline the acceptable use of computer equipment and the associated services within ARK. These rules are in place to protect both the employee and ARK because inappropriate use exposes us all to unnecessary risk.

3.0 Scope

3.1 This policy applies to all employees, contractors, consultants, temporary employees, other workers at ARK and the academies and overseas employees including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by ARK.

4.0 General Use and Ownership

4.1 While ARK seeks to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of ARK. The need to comply with legislation or to protect ARK means that management cannot guarantee the confidentiality of

information stored on any network device belonging to ARK.

4.2 ARK reserves the right to audit equipment, systems and network traffic on both a periodic basis or randomly to ensure compliance with this policy. This includes email (both inboxes and other folders); the hard drives of individual devices and user areas on networked devices.

4.3 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor or manager.

4.4 ARK recommends that any information that users consider sensitive or vulnerable be encrypted. For advice and support in this regard users should contact ARK IT through the following channels:

1. Email using ithelpdesk@arkonline.org;
2. Call ext 1789; or
3. Use the website http://servicedesk.arkonline.org

5.0 Security and Proprietary Information

5.1 Users must keep passwords secure in accordance with the Password Policy and should not share account details with anyone. This includes family and other household members when work is being done at home.

5.2 Employees must use caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojans. Any concerns in this regard should be reported immediately to ARK IT through the Service Desk as detailed above in para 4.4.

6.0 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

6.1 Engaging in any activity that is illegal under local, national or EU legislation and / or statute (no exceptions);

6.2 Undertaking deliberate activities that waste the effort and time of ARK IT and/or network resources;

6.3 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by ARK;

6.4 Unauthorised copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which ARK, or the end user does not have an active license;

6.5 The intentional introduction of malicious programs into the network or server (e.g., viruses, worms, Trojans, email bombs, etc.);

6.6 Revealing your account password to others or allowing use of your account by others;

6.7 Making fraudulent offers of products, items, or services originating from any ARK account;

6.8 Making statements about warranty, expressly or implied, unless it is a part of normal job duties;

6.9 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;

6.10 Port scanning or security scanning is expressly prohibited;

6.11 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty;

6.12 Circumventing user authentication or security of any host, network or account;

6.13 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack);

6.14 Using any programme/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet / Intranet / Extranet;

6.15 Using an ARK asset to view, create, distribute or conceal any material that is obscene, hateful, or pornographic or is contradictory to the values inherent in ARK's work as a children's charity;

6.16 Attempting to circumvent ARK's internet filtering solution;

6.17 Providing information about, or lists of, ARK employees to parties outside ARK;

6.18 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam);

6.19 Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages;

6.20 Unauthorized use, or forging, of email header information;

6.21 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies;

6.22 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type;

6.23 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam);

6.27 Revealing any confidential or proprietary information, trade secrets or any other material deemed confidential by ARK. Employees should also be mindful of the obligations under the Data Protection Act (1998) and associated legislation and guidance;

6.28 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, ARK trademarks, logos and any other ARK, intellectual property may also not be used in connection with any social networking activity;

6.29 Utilising ARK resources to conduct any commercial or voluntary business unrelated to ARK;

6.30 Utilising ARK systems for the purposes of gambling for financial gain;

6.31 Utilising ARK resources during working hours for any non-work related activity that impacts on the ability of the staff member to carry out their duties.

7.0 Use of Social Networking

7.1 Use of social networking sites or functions by employees, whether using ARK property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of ARK systems to engage in social networking is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate ARK policy, is not detrimental to ARK's best interests, and does not interfere with an employee's regular work duties. Use of social networking from ARK systems is also subject to monitoring at the discretion of the IT Director.

7.2 Employees shall not engage in any social networking or online activities that may harm or tarnish the image, reputation and/or goodwill of ARK and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when using social networking sites or otherwise engaging in any conduct prohibited by ARK's Dignity at Work Policy.

7.3 Employees may also not attribute personal statements, opinions or beliefs to ARK when engaged in social networking. If an employee is expressing his or her beliefs and/or opinions on social networking sites, the employee may not, expressly or implicitly, represent themselves as an employee or representative of ARK. Employees assume any and all risk associated with social networking.

8.0 Professional Responsibilities for Users in Schools or interacting with pupils in ARK Schools.

8.1 Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies;

8.2 Do not talk about your professional role in any capacity when using social networking tools;

8.3 Do not put online any text, image, sound or video file that could upset or offend any member of the whole school community or be incompatible with your professional role;

8.4 Use school IT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera;

8.5 Do not give out your own personal details, such as personal mobile phone number, personal email address or social network details to pupils, parents and carers;

8.6 Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately;

8.7 Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT;

8.8 Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory;

8.9 Ensure that your online activity, both in school and outside school, will not bring your organisation or professional role into disrepute;

8.10 You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation appropriately.

9.0 Enforcement

9.1 Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Name: _____

Signature: _____

Date: _____