IT POLICY

Date of last review:	**November 2015**	**Review period:**	**3 years**
Date of next review:	**November 2018**	**Owner:**	**IT Director/CIO**
Type of policy:	**Network**	**LGB/Board/Other approval:**	**Risk and Audit Committee**

IT Policy

Table of Contents

1. Purpose

This document outlines, for all Ark school staff, our policy on Information Technology and its use.

2. How to use this Policy

This policy document embodies all current aspects of IT use at Ark. Section 6 and 7 deal with general aspects of the Acceptable Use of IT at Ark and Data Security and Data Transfer in broader terms.

Subsequent sections deal with Passwords, Securing Data, Sharing Data, "Bring-Your-Own" and Mobile devices.

3. Scope and definition

The policy applies to all Ark school staff and trustees of Ark schools as well as to volunteers, local governors, and to contractors/consultants when engaged on Ark school business (known as "Ark school staff").

The Policy covers the use of IT by any member of Ark School Staff, password obligations, data security obligations, and acceptable use obligations relating to the use of Computers and personal devices (tablets, smartphones and mobile telephones) by any member of Ark School Staff whilst engaged on Ark school business.

This policy also consolidates and replaces the following existing policies:

MOBILE PHONE SECURITY POLICY (November 2011)
IT PASSWORD POLICY (November 2011)
BRING YOUR OWN DEVICE POLICY (July 2013)
IT ACCEPTABLE USE POLICY (April 2012)

Any potential breaches of any aspect of this IT policy may be investigated and could result in disciplinary action, up to and including dismissal.

4. Principles of this Policy

All Ark Staff need to be aware of the rules and standards applied by Ark Schools regarding the use of IT or any resources involving IT. IT must be used appropriately; its use must always minimise risk to Ark Schools' operations, and also ensure that the sensitive nature of the data we deal with is protected and secured as a priority.

5. Context of this Policy

- IT enables access to, storage of and the transmission of data. Much of the data we access is very sensitive as it relates to our pupils and their education. So we must ensure that access, storage and transmission of that data is always conducted with care in order to protect and safeguard it.

- Today's IT systems and the personal devices we are increasingly using in business enable significantly easier access to data, and also a far greater ability to share data. But with this comes the need for increased awareness around protecting data that is in any way sensitive.

- It is important to understand and be aware that data is always "stored" somewhere, and can be moved or shared via email or through the use of some of the many "apps" that are now available on portable devices. It is the responsibility of Ark school staff to be continually mindful of where sensitive data is stored (particularly if on portable or personal devices) and how sensitive data is being shared (i.e. by email or using other collaborative technologies), and to take steps to protect that data in every scenario.

- This policy states how Ark school staff should act in the areas of Data Security, Password protection, Data sharing, in the acceptable use of IT and when using Mobile phones and Personal Devices.

- Prevent Duty. The statutory guidance makes clear the need for schools and staff to ensure that children are safe from terrorist and extremist material when accessing the Internet in schools. Schools should ensure that suitable filtering is in place. More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on Internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, every teacher and member of staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

6. The Acceptable Use of IT

This section is not intended to impose restrictions that are contrary to Ark's 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.

All information technology assets procured or funded by Ark including but not limited to computer equipment, software, operating systems, storage media, network accounts providing email, WWW browsing, and Internet Explorer are the property of Ark and are governed by the conditions in this section. These

systems are to be used for business purposes in serving the interests of the organisation.

Section 6.6 “Professional Responsibilities” covers the use of information technology assets in any capacity whether they are procured or funded by Ark or part of the user’s domestic or personal provision.

Acceptable and appropriate use is to be considered a team effort involving the participation and support of every member of Ark staff. It is the responsibility of every user to observe and implement these guidelines, and to conduct their activities accordingly.

6.1. Context

This section outlines the acceptable use of computer equipment and associated IT associated services within Ark. These rules are in place to protect both employees and Ark because inappropriate use exposes us all to unnecessary risk.

6.2. Who does this apply to?

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

6.3. General Use and Ownership

While Ark seeks to provide a reasonable level of privacy, users should be aware that the data they create on Ark 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.

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

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.

Ark recommends that any information that users consider sensitive or vulnerable be encrypted. For advice and support in this regard users should contact their Line Manager, and, if required, the Civica Help Desk.

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

Employees must exercise caution when opening email attachments received from unknown senders, which may contain viruses, email phishers, or Trojans. Any concerns in this regard should be reported immediately to the Civica Help Desk.

6.4. Unacceptable Use

The following activities are, in general, prohibited. Employees may occasionally 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).

- Engaging in any activity that is illegal under local, national or EU legislation and / or statute (no exceptions)
- Undertaking deliberate activities that waste the effort and time of the Civica Support team and/or network resources
- 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
- Unauthorized 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
- The intentional introduction of malicious programs into the network or server (e.g. viruses, worms, Trojans, email bombs, etc.)
- Revealing your account password to others or allowing use of your account by others
- Making fraudulent offers of products, items, or services originating from any Ark account
- Making statements about any form of guarantee, expressly or implied, unless it is a part of normal job duties
- 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
- Port scanning or security scanning is expressly prohibited
- 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
- Circumventing user authentication or security of any host, network or account
- Interfering with or denying service to any user other than the employee's host (for example, instigating a denial of service attack)

- 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
- 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
- Attempting to circumvent Ark's internet filtering solution
- Providing information about, or lists of, Ark employees to parties outside Ark
- 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)
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages
- Unauthorized use, or forging, of email header information
- 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
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam)
- 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 (these obligations can be reviewed HERE).
- 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 these may also not be used in connection with any social networking activity
- Utilising Ark resources to conduct any commercial or voluntary business unrelated to Ark
- Utilising Ark systems for the purposes of gambling for financial gain
- 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.

6.5. Use of Social Networking

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/CIO.

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.

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.

6.6. Professional Responsibilities for Users in Schools or Users interacting with pupils in Ark Schools.

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies
- Do not talk about your professional role in any capacity when using social networking tools
- 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
- Use school IT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera
- 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
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately
- Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Ensure that your online activity, both in school and outside school, will not bring your organisation or professional role into disrepute
- You have a duty to report any e-Safety incident that may impact on you, your professionalism or your organisation appropriately.

7. Keeping Data Secure and Sharing Data

The following security measures are mandated to secure sensitive data pertaining to pupils and staff whether held by any central system or in any central location, being transferred between schools and any central system, or located on any portable device.

7.1. Physical access to data

- Staff in all instances must responsibly manage any Ark-related Data on staff laptops or portable devices.
- Any sensitive data should not normally be retained on any laptop or portable device, unless it is fully protected from unauthorised access using Ark username and password credentials.
- In the event that a laptop or portable device is mislaid, it is the responsibility of the staff member to inform the Civica Help Desk of such loss so that they can take steps to minimise further access attempts to that device by any 3rd party, and subsequently attempt to perform a procedure to remotely erase any and all data on that device.
- Where data is held in development environments, backups, or testing environments, all staff involved must encrypt hard drives so if equipment is lost, the information cannot be retrieved. Any contractor or consultant working with Ark and utilising Ark data is instructed to delete all such data at the end of the contract.
- Backups are taken from systems and are stored within an internal IT shared area that is not encrypted, and as such are protected from external access. Such backup data is only accessible to restricted members of Ark staff.
- All Ark-owned software (e.g. CCR! source code) is managed on the Github external repository, which uses HTTPS (an industry standard encryption protocol used over the Internet) and is password protected.
- Information that is held outside (e.g. CCR! in the cloud, Tableau) Ark's protected infrastructure is managed on OVH's (a 3rd party ISP used by the Systems and Data team) infrastructure, which complies with industry standard regulations, including restriction of physical access to servers. Further, all data held on the virtual servers at this location is encrypted on this 3rd party infrastructure.
- Any data held within the new O365 environment is encrypted "de facto".
- Physical access to databases e.g. HR, Recruitment, Finance is controlled using SQL Server authentication mechanisms, which is fully auditable. This server is within Ark's internal infrastructure and so it is also protected within Ark's internal network.

7.2. Data transfer

- Data that is sent internally for development purposes via email (from one member of staff to another) is not encrypted, as it is always transferred within Ark's own internal email infrastructure and does not enter the public email system.
- If sensitive data is sent to an external email address, it must be sent within an encrypted container (e.g. a zip file) and a password must be provided separately using another method (e.g. SMS). Any member of staff within the Ark Network must ensure that this or other appropriate encryption is applied when sending email from a Network address to an

email address outside of the Ark Network, as the public email system is not secure.

- General email traffic in and out of Ark is normally sent and received via LGFL (a widely used email transport infrastructure within the Education sector) that also provides filtering of email. However, it must still be the responsibility of any member of Ark Network staff to ensure that they transfer any sensitive data via email in a protected fashion.
- Bulk data (for example pupil data used for analysis purposes) is moved to and from schools using the MPLS cloud, or another similarly secure VPN tunnel (a mechanism used to create a private and secure link between different systems over the public Internet).
- Student data transfer to the centre is enabled via the HTTPS protocol (a mechanism that uses a key to encrypt data transfer over the public Internet, commonly used, for example, in banking transactions) and additionally protected with usernames and passwords.

7.3. Data access

- CCR! has restricted access and access is only allowed by explicitly adding the staff member to an "Active Directory" (AD security group. This can only be performed by an Administrative user who has the rights to update Active Directory in this way. Otherwise, access is not provided. All access to all CCR! Reports (from 2010) are logged and auditable.
- Access to all Source Code and Ark Software Intellectual Property is username and password protected.
- Access to Ark's MIS system is username and password protected and is only possible within the internal Ark network. These passwords also expire regularly, and must therefore be pro-actively changed.
- Access to the network to further access the MIS is username and password protected and follows the Password policy described in section 8 of this policy. Depending on the site, passwords expire frequently and must therefore be pro-actively changed.
- Access to the HR Recruitment system is username and password protected and all access is logged.
- Access to the HR system is username and password protected.

7.4. Summary

Ark's data is either encrypted at its storage location, or is held within our own internal protected environment. Access to such data can only be gained if anyone seeking access has a network username and password as well as a system username and password.

It is therefore a condition of employment that any member of Ark Network staff:

- Ensure that any sensitive data is only held on any portable device if such data is protected using encryption or appropriate username and password credentials.

- Ensure that any sensitive data sent via email or any other transfer method that relies on the public Internet be appropriately protected via an encryption method.
- Ensure that sensitive data is not retained on any portable device without appropriate protection in the event of loss of such device.
- Ensure that the loss of any portable device used for any activities relating to Ark be immediately reported to the Civica Help Desk.

8. Passwords

8.1. Context

Passwords are an important aspect of computer security. They are the “front line” of protection for all Ark user accounts. A poorly chosen password may result in the compromise of our entire enterprise network. As such, all Ark staff (including contractors and vendors with access to Ark systems) are responsible for taking the appropriate steps outlined below to create and secure their passwords. The following is a minimum standard for the creation of strong passwords, the protection of those passwords, and the frequency of change of passwords.

8.2. Who does this apply to?

The use of Passwords applies to all personnel who have or are responsible for an IT User account (or any form of access that supports or requires a password) on any system that resides at any Ark facility, has access to the Ark network, or stores any non-public Ark information.

8.3. General rules relating to Passwords

All system-level passwords (e.g. root, enable, system admin, application administration accounts, etc.) must be changed on at least a 60-day basis.

8.4. Changing Passwords

All user-level passwords (e.g. email, web, O365, desktop computer, etc.) must be changed at least every 60 days. Users will be prompted to do so when logging on. You will be prevented from re-using your previous 6 passwords. If a user forgets their password Civica can reset it. If this is required please contact your local Civica support team.

8.5. Passwords associated with System-level privileges

User accounts that have system-level privileges granted through group memberships (or programs such as "sudo") must have a different and unique password from any other account held by that user.

8.6. Protecting Passwords

Passwords must not be inserted into email messages or other forms of electronic communication. When sending password protected files via email do not send the password via the same medium. Instead communicate the password via an alternative method. For example, use the telephone or text message as appropriate.

8.7. Protecting Passwords (relating to email transmission protocols)

Where SNMP is used (SNMP being a base-level protocol used to send email), the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g. SNMPv2). If further assistance is required around this requirement, please contact the Civica Help Desk, but if you are using an Ark email client (Outlook, for example) you do not need to be concerned as to this requirement, as the email client does not make use of SNMP.

8.8. Password Creation Standards

User passwords must be at least ***eight characters long and be alphanumeric i.e. contain both letters and numbers***. For the avoidance of doubt, each password must contain at least one number and at least one letter and the letter/s can be either upper or lower case.

Everyone should be aware of how to create strong user passwords. As such, following are some guidelines for the creation of passwords.

Poor or weak passwords have the following characteristics:

- The password contains less than fifteen characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Is not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

- Passwords should never be written down or stored online. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Users are required to adhere to following rules when generating passwords:

- Do not use the same password for Ark user accounts as for other non-Ark access (e.g. personal ISP account, option trading, benefits, etc.)
- Do not share Ark user passwords with anyone, including administrative assistants or PAs. All passwords are to be treated as sensitive, confidential Ark information.
- Don't reveal a user password over the phone to ANYONE
- Don't reveal a user password in an email message
- Don't reveal a user password to your manager
- Don't talk about a password in front of others
- Don't hint at the format of a user password (e.g. "my family name")
- Don't reveal a user password on questionnaires or security forms
- Don't share a user password with family members
- Don't reveal a user password to co-workers while on vacation
- Do not use the "Remember Password" feature of applications.
- Do not write user passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system or mobile device without encryption.
- If a user account or user password is suspected to have been compromised, change the Password and then report the incident to the Civica Help Desk immediately.
- Attempts at User password cracking or guessing may be performed on a periodic or random basis by Ark IT support or its delegates. If a user password is guessed or cracked during one of these scans, the user will be required to change it.

8.9. Application Development Standards relating to Passwords

Application developers must ensure their programs contain the following security precautions:

Applications should support authentication of individual users, not groups. Applications should not store passwords in clear text or in any easily reversible form.

Applications should provide for some form of role management, such that one user can take over the functions of another without having to know the other's password.

9. Ark-issued Mobile Phones and Mobile devices

9.1. Context

This Section defines the conditions under which Ark-owned and issued mobile phones and devices may be used to access Ark Email, Calendar, Tasks and Contacts and all other Ark systems and IT Services.

Ark may provide Blackberry devices, iOS devices and Windows devices and associated services for exclusive use of its employees to assist in the performance of their duties. Ark wishes to encourage the security standards articulated in this section to safeguard employees, protect Ark assets and ensure compliance with appropriate legislation.

Individual deviations from and exceptions to the conditions in this section will be dealt with on a case-by-case basis and users are required to demonstrate the business need relevant to any deviation or exception.

9.2. Who does this apply to?

These conditions apply to all Ark Staff, and to sub-contractors engaged in any Ark business, who have been issued a Mobile device (SmartPhone or Tablet) by Ark.

Should a user wish to pursue a deviation or exception to the conditions within this section then please contact your Manager in the first instance.

9.3. Usage

Usage of Ark-issued devices is as defined in 10.4, 10.5 and 10.7 of this document.

9.4. Securing Ark-issued devices

Security stipulations are as defined in Section 10.4 of this document.

9.5. Use of 3rd Party applications ("Apps")

The downloading and use of any 3rd party apps is not generally permitted.

- Ark cannot test the impact that every available app would have on an individual device, the overall solution or our wider network.

- However, if there is a clear business need for an application a request with justification, approved in writing by a Line Manager, should be sent to the Civica Help Desk.

10. Personal Devices ("Bring Your Own Device" or BYOD)

10.1. Context

This Section defines the conditions under which personally owned devices may be used to access Ark Email, Calendar, Tasks and Contacts and all other Ark systems and IT Services. These conditions enable the use of personally owned devices to assist staff in the performance of their duties whilst protecting the security and integrity of Ark's data and technology infrastructure.

10.2. Who does this apply to?

These conditions apply to all Ark Staff, and to sub-contractors engaged in any Ark business.

All users wishing to access Ark resources using personal devices will be required to abide by these Conditions. If you do not wish to be subject to these conditions of use, then you should rather seek to use an Ark-issued portable device rather than your own.

10.3. Definition of "Personal Devices"

The "Personal Devices" to which this Section relates include (but are not limited to) the following:

- Android Smartphones, Tablets and other Android-based devices
- Blackberry Smartphones, Playbooks and other Blackberry-based devices
- iOS iPhones, iPads and other iOS-based devices
- Windows Smartphones, Tablets and other Windows-based devices

By definition, such "Personal Devices" are deemed to be devices that are the personal property of the user, rather than devices issued to the user by Ark.

10.4. Securing "Personal Devices"

Ark reserves the right to disconnect devices, disable services and "wipe" devices without notification, when these devices are being used for Ark business.

Users must ensure that a 4 or 6 digit PIN is set up on their device to unlock the device prior to using it.

The PIN must be set by the user and not shared with anyone.

Users are expected to change their PIN at least every 60 days.

Any member of Staff using a personally-owned device for anything related to Ark Business must ensure that the device is appropriately secured as per these guidelines and must take full personal responsibility for ensuring the security of any data related to Ark business on that device.

10.5. User Responsibilities for the Ark-related use of "Personal Devices"

The user agrees that (and takes full responsibility for ensuring that) the device will have any Ark business-related data removed from the device when they leave Ark, when the device is given / sold to someone else, when the device is lost or stolen, when the device is sent for warranty repair or loaned to any 3rd party.

It is therefore the user's responsibility to take additional precautions to prevent the loss of personal data, such as backing up messages, contacts etc.

Members of staff are responsible for notifying their mobile carrier upon loss of the device (as the device is the property of the staff member rather than Ark).

Users are personally liable for all costs associated with their device.

Users are responsible for managing work calls and how they are charged back to Ark.

Users assume full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

Users agree to keep the operating system up to date and keep the device current with security patches and updates, as released by the manufacturer.

Users will not 'Jail Break' the device (installing software that allows the user to bypass standard built-in security features and controls).

Users agree that the device will not be shared with other individuals or family members, due to the business use of the device.

Users agree to delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing e-mail attachments.

10.6. Support for "Personal Devices"

Ark (via its IT Service Delivery Partner Civica) only supports devices that are provided through the business by Ark. Personally owned devices will not be supported. It will be the responsibility of the user to connect their personal device to the Ark domain and ensure that connection is appropriately maintained.

10.7. Use of "Personal Devices" in line with current Legislation

All mobile 'phone users should refer to the Royal Society for the Prevention of Accidents guidelines on the use of mobile phones whilst driving. (These guidelines can be reviewed in detail HERE.

This code of practice will be amended from time to time in response to changing circumstances and operational and legislative requirements. As a condition of use, it is the responsibility of users to ensure that they keep up-to-date with the latest requirements of the document.

The use of any Personal Device whilst being used for Ark business of any description must be conducted in line with current legislation.

10.8. Authorisation for the use of "Personal Devices" for Ark Business

In order to access Ark resources on a personal device, written confirmation must be provided by a Line Manager.

10.9. Enforcement

Any member of Ark Staff found to have violated BOYD use policy may be subject to disciplinary action, up to and including termination of employment.

11. Replaced Policies and Forms

This Policy replaces those detailed in Section 3.

12. Changes to this Policy

Ark Schools reserves the right to make changes to this policy at any time.

13. Queries relating to this Policy

If you have any queries relating to this policy, please contact your line manager who may escalate your query to the Principal or Ark Schools CIO, as relevant.