ONLINE SAFETY & ACCEPTABLE USE POLICY FOR STAFF AND STUDENTS

Last Review Date	August 2025
Next Review Date	August 2026
Version	V1.14/08/25
Policy Reviewer	Director – Kane Wilson

INTRODUCTION

The policy defines and describes the acceptable use of ICT (Information and Communications Technology), all mobile devices for centre-based employees and ensuring all staff are aware of their responsibilities with the growing use of social networking sites. Its purpose is to minimise the risk to students for inappropriate contact from staff, to protect employees and schools from litigation and to minimise the risk to ICT systems.

POLICY STATEMENT

The Ark Smallholding recognises the use of its ICT and communications facilities as an important re source for teaching, learning and personal development and as an essential aid to business efficiency. It actively encourages staff to take full advantage of the potential for ICT and communications systems to enhance development in all areas of the curriculum and school administration. It is also recognised by the directors that along with these benefits there are also responsibilities, especially for ensuring that children are protected from contact with inappropriate material.

In addition to their normal access to the company's ICT and communications systems for work related purposes, the directors permit staff limited reasonable personal use of ICT equipment and email and internet facilities during their own time subject to such use:

- not depriving pupils of the use of the equipment and/or
- not interfering with the proper performance of the staff member's duties

Whilst the company's ICT systems may be used for both work-related and for personal use, the direc tors expect use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of The Ark Smallholding at all times.

This policy document is to be issued to all staff on its adoption by the directors and when new staff are provided with mobile phones and passwords giving access to the ICT network.

POLICY COVERAGE

This policy covers the use by staff of ICT and communications equipment both provision owned and for personal use: examples of which include:

- laptop and personal computers
- ICT network facilities
- personal digital organisers and handheld computers
- mobile phones and phone/computing hybrid devices
- Flash drives and other physical and on-line storage devices
- Image data capture and storage devices including cameras, camera phones and video equipment

This list is not exhaustive.

WHO DOES THE POLICY APPLY TO?

This policy applies to all company staff employed by the The Ark Smallholding, staff that are employed through agencies and volunteers. It also applies to learners who are currently enrolled to at tend the provision.

AIMS OF THE POLICY

Ensure that employees and others listed above are aware of the risks associated with the inappropriate use of social networking sites and understand the importance of using them safely and securely.

Safeguard employees and others listed in the section above to ensure they do not make themselves vulnerable through their use of social networking sites.

Ensure that The Ark Smallholding maintains its duty to safeguard children, staff, the reputation of the Company, the wider community and the Local Authority.

RELEVANT LEGISLATION

The Human Rights Act 1998

Data Protection Act 1998

Freedom of Information Act 2000

Computer Misuse Act 1990, updated by the Police and Justice Act 2006

Regulation of Investigatory Powers Act 2000 (RIPA)

THE USE OF THE ARK SMALLHOLDING ICT AND COMMUNICATIONS FACILITIES

USE OF THE ARK SMALLHOLDINGS ICT EQUIPMENT

Staff who use the company's ICT and communications systems:

- must use it responsibly
- must keep it safe
- must sign and agree to the terms of the loan agreement (see appendix 1)
- where any damage/loss has occurred, the user is responsible for the replacement cost
- must not share and must treat as confidential any passwords provided to allow access to ICT equipment and/or beyond firewall protection boundaries
- must report any known breach of password confidentiality to the Director or nominated ICT Technicians as soon as possible
- must report known breaches of this policy, including any inappropriate images or other mate rial which may be discovered on the company's ICT systems
- must report to the Director any vulnerabilities affecting child protection in the company's ICT and communications systems
- must not install software on the company's equipment, including freeware and shareware. • must comply with any ICT security procedures governing the use of systems in the centre, including anti-virus measures
- must ensure that it is used in compliance with this policy

Any equipment provided to a member of staff is provided for their personal use. Any use of the equipment by family or friends is not permitted and any misuse of the equipment by unauthorised users will be the responsibility of the staff member.

Whilst it is not possible to cover all eventualities, the following information is published as guidance for staff on the expectations of the The Ark Smallholding. Any breaches of this policy or operation of the company's equipment outside statutory legal compliance may be grounds for disciplinary action being taken.

EMAIL AND INTERNET

The following uses of the company's ICT system are prohibited and may amount to gross misconduct and could result in dismissal:

- to make, to gain access to, or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it
- to make, to gain access to, and/or for the publication and distribution of material promoting homophobia or racial or religious hatred
- for the purpose of bullying or harassment, in connection with discrimination or denigration on the grounds of gender, race, religious, disability, age or sexual orientation
- for the publication and/or distribution of libellous statements or material which defames or de grades others
- for the publication of material that defames, denigrates or brings into disrepute the centre and/or its staff and pupils
- for the publication and distribution of personal data without authorisation, consent or justification

- where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination
- to participate in on-line gambling
- where the user infringes copyright law
- to gain unauthorised access to internal or external computer systems (commonly known as hacking)
- to create or deliberately distribute ICT or communications systems “malware”, including vi ruses, worms, etc.
- to record or monitor telephone or email communications without the approval of the Director. In no case will such recording or monitoring be permitted unless it has been established for that such action is in full compliance with all relevant legislation and regulations (see Regulation of Investigatory Powers Act 2000, below)
- to enable or assist others to breach the directors expectations as set out in this policy

Additionally, the following uses of school ICT facilities are not permitted and could lead to disciplinary action being taken:

- for participation in “chain” e-mail correspondence (including forwarding hoax virus warnings)
- in pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade unions)
- to access ICT facilities by using another person’s password, or to post anonymous messages or forge e-mail messages using another person's identity

USE OF SOCIAL NETWORKING SITES, EMPLOYEES, VOLUNTEERS AND DIRECTORS

INTRODUCTION

The Company is committed to ensuring that all staff are aware of their responsibilities in connection with the growing use of social networking sites such as blogs, Facebook, Snapchat, Youtube, Windows Live Spaces, Tiktok, forums, Instagram, Twitter, bulletin boards, multiplayer online gaming, chatrooms and instant messenger. Please note that this is a non-exhaustive list for illustrative purposes only and it should not be assumed that if it does not appear on this list the policy does not apply.

RESPONSIBILITIES AS EMPLOYEES

Staff are expected to maintain professional boundaries with pupils and there should be a clear separation of the private social lives of staff and that of pupils. Staff are advised that it is inappropriate to have on-line relationships with pupils (except where appropriate within family relationships) or to allow pupils access to their own pages. Similarly accessing pupils’ pages is discouraged as this may cross the professional boundary that should be maintained between staff and pupils.

Employees:

- should not befriend pupils online as personal communication could be considered inappropriate and may potentially make them vulnerable to allegations.
- should not place inappropriate photographs on any social network space.
- should not post indecent remarks.

- if a message is received on their social networking profile that they think could be from a pupil they should report it to their Line Manager/Director so that this can be investigated, and the appropriate action taken.
- must not disclose any confidential information or personal data about any individual/pupil/colleague which could be in breach of the Data Protection Act.
- should not post photographs or comments about pupils, other colleagues, the company, parents/guardians on social networking sites.
- should not make defamatory remarks about the company/colleagues/pupils/parents/guardians or the Local Authority or post anything that could potentially bring the company or the Local Authority into disrepute.
- should be aware of the potential for on-line fraud and should be cautious when giving out personal information about themselves which may compromise their personal safety and security.
- should not access social networking sites for personal use via company information systems or using company equipment.
- staff should set their Social Network (facebook) settings to the maximum. For guidance on how to do this please see, Using Facebook Safely, a Guide for Professionals Working with Young People.

MOBILE DEVICES

Staff use of mobile phones during their working day should be:

- Outside of their contracted hours
- Discreet and appropriate e.g. not in the presence of pupils
- Staff should not make or take personal calls or engage in personal texting during works time.
- Staff should never contact pupils or parents from their personal mobile phone or give their mobile phone number to pupils or parents.
- Staff should not use their mobile phones on the corridors, student social areas or in class rooms (during the school day)
- Staff are advised not to make use of students' mobile numbers either to make or receive phone calls or to send to or receive from students' text messages other than for approved company business.
- Staff should only communicate electronically with students from school accounts on approved company business, e.g. coursework
- Staff should not enter into instant messaging communications with students.

Note: The above restrictions apply to the use of phones, e-mails, text messaging, internet chatrooms, blogs, and personal websites (including personal entries on Facebook etc).

BREACHES OF THE POLICY

In instances where it is alleged that an issue has arisen in connection with the use of social media the following will apply:

Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure or other appropriate procedure.

The Governing Body will then take appropriate action in order to protect the centres reputation and that of its staff, parents, governors, children and anyone else directly linked to the company. Certain breaches may lead to your contract of employment or other agreed terms of engagement being subject to summary termination.

Under the Regulation of Investigatory Powers Act 2000 (RIPA), the company can exercise the right to monitor the use of the company's information systems and internet access where it is believed that unauthorised use may be taking place, to ensure compliance with regulatory practices, to ensure standards of service are maintained, to prevent or detect crime, to protect the communications system and to pick up messages if someone is away from company. If such monitoring detects the unauthorised use of social networking sites disciplinary action may be taken where appropriate.

ACCEPTABLE USE BY LEARNERS

All learners enrolled with The Ark must follow the Company guidelines set out below:

- To hand in all electronic devises after entering the building
- Use computers for educational purposes only
- Access only information on the internet that would be acceptable in the centre in written form
- Understand that the use of social networking sites are not permitted within the centre
- To use acceptable language in all documents produced
- Use all computers safely and with common sense
- Access to Google and YouTube is only permitted with approval from a tutor
- Report any concerning or offences words or imagery
- Accept that the Director may check computer files, monitor internet site use and record computer activity
- The use of personal data files is not permitted

TRAINING FOR STAFF

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
- Abusive, threatening, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and any deputies will undertake child protection and safeguarding training regularly. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

SECURITY PROCEDURES

The directors will be responsible for:

- Putting in place an appropriate level of security protection procedures, including filtering and monitoring systems on devices and networks used by staff and students, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at The Ark, including terrorist and extremist material
- Ensuring that the IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting daily, weekly and termly checks to ensure the IT systems are updated and providing protection for end users.

ESCALATION PROCESS

Procedures for dealing with online-safety concerns or incidents will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including academy sanctions)
- PREVENT - Risk Assessment / Policy

- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Colleague Code of Conduct

The Ark Smallholding commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside the centre and outside (and that incidents outside The Ark may continue to impact pupils when they come into The Ark or during extended periods away). All members of The Ark are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day.

Actions where there are concerns about a child:

Staff should follow the Safeguarding and Child Protection policy if they are concerned about the safety of a pupil at The Ark and report their concerns to the DSL of the host school using CPOMS.

Sexting - sharing nudes and semi-nudes:

Staff should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Colleagues other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The academy DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.