Acceptable Use Policy

This Policy was developed and approved by Action for Children for internal use. It is believed to be an accurate reflection of the legislation and other relevant regulatory requirements at the time it was approved. It should not be incorporated into or used by other organisations without permission. Action for Children is committed to the safeguarding of children and young people, staff, volunteers.	
Policy Name:	Acceptable Use Policy
Document Name:	Acceptable Use Policy
Document Type:	Policy
Policy Area:	Technology
Owner:	Director of Technology
Approved by:	Stuart Harper
Current Contact:	Richard Hill
Date Issued / Last Updated:	10th July 2020
Latest Date to be re-updated and reapproved:	9th July 2023

Document Controls:

Version	Author	Date of Issue	Reason for Issue
1.31	Richard Hill	18/09/2020	4.18.3 added re existing peripherals and WVD removed 4.4.3
1.32	Richard Hill	16/11/2020	Minor amendment to 4.24 as requested by M. Guilfoyle. 4.4.8 added re mobile SIMs. 4.8.4 added re not storing files on the local hard disk.
1.33	Richard Hill	19/05/2021	4.6.4 added regarding approved organisational devices and applications.
1.34	Richard Hill	15/07/2021	4.6.6 added relating to taking photos and 4.6.15 updated. 4.7.5 – 4.7.7 added relating to data.
1.35	Richard Hill	04/08/2021	4.22.2 amended to IT Security Manager
1.4	Richard Hill	08/09/2021	Amendments to align with the Encryption Standards Policy and Cloud & Network Security Policy. Also 4.7.18 added and 4.13.2 removed.
1.41	Richard Hill	08/11/2021	Update to Password Policy 4.2.2 and 4.2.3
1.42	Richard Hill	15/11/2021	Amended 4.23.2 to include Ireland.
1.43	Richard Hill	22/12/2021	Amendment to 4.4.1 to allow biometrics to be used on AFC phones
1.44	Richard Hill	06/12/2022	Added 4.5 Cameras and amended 4.6 Portable Devices

Contents

1. Purpose

Action for Children is committed to the safe care of children, young people and their families. The safe use of information and telecommunication technologies is a vital part of this. The inappropriate use of IT, as outlined in this policy, the Data Security Policy and Social Media policy is a breach of the organisation's Code of Conduct.

All users must use the IT and telephony services efficiently in a secure and legally compliant manner in line with the Data Protection Act 2018, the Computer Misuse Act 1990 and all other relevant legislation.

The aim of this policy is as follows:

- Outline the acceptable use of its information systems and data.
- Protect Action for Children, its employees and volunteers.
- To promote the professional, ethical, lawful and productive use of Action for Children information systems.
- To define and prohibit unacceptable use of Action for Children information systems.
- To educate users about their information security responsibilities.
- To describe where, when and why monitoring may take place.

An information system, for the purposes of this policy is defined as 'anything used for collecting, storing, and processing data and for providing information, knowledge, and digital products.'

For the purposes of this policy, a personal device is defined as any mobile phone, smartphone, laptop or tablet which has been purchased by an individual and is their property and is not owned by Action for Children.

Proper use of devices reduces the risk of introducing malware (such as ransomware), hackers and data breaches that can cause reputational damage to Action for Children, affecting our ability to provide care to children.

In general, acceptable use covers everything including respecting the rights of other computer users, the integrity of the physical facilities, and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, Action for Children may take disciplinary action, up to and including suspension or termination of employment.

Employees and users understand that any communications sent or received via Action for Children systems and devices, whether by email, internet, telephone or any other method will be processed by Action for Children as detailed in the Internal Privacy Notice.

Action for Children can access, review, log, copy, delete, investigate or audit any systems access and messages, and will do so as required for the operation of the charity, as detailed in the Internal Privacy Notice. This may result in this information being disclosed to persons outside of Action for Children if it is deemed appropriate and or necessary, as detailed in the Internal Privacy Notice.

It is therefore good practice to not use the internal IT resources and communications systems for any matter that is unrelated to Action for Children and that the user requires to be kept private and/or confidential from Action for Children.

If a user is employed or engaged by Action for Children, they are expected to read, understand and comply with this policy as an important requirement of their ongoing employment or engagement. If a user is in any doubt and requires clarification on any point, they should contact their line manager.

2. Scope and Audience

The scope of this policy applies to all devices and assets that are owned or leased by Action for Children, and other equipment that may be used to access Action for Children's systems including personal devices.

Devices are defined as any equipment that can access the internet, store or transmit data and documents, this includes but is not limited to, mobile phones, SIM cards, laptops, desktops, tablets, USB sticks, memory cards, cameras and GPS.

Assets are defined as any data, device, or other component of the environment that supports information-related activities and has a value to Action for Children. (Value may be financial or be relevant to the reputation of Action for Children). Assets include databases, electronic file storage, web platforms as well as documents, filing cabinets and premises.

This policy applies to all workers, employees, contractors, consultants, and temporary employees and volunteers of Action for Children and its group companies, including all personnel affiliated with third parties that use Action for Children's information systems. References to 'Action for Children' below may be read as reference to the relevant Action for Children group company or companies, in context, accordingly.

Users are defined as employees, contractors, sub-contractors, service users, guests and anyone else that intends to or has access to Action for Children's information systems.

3. Terminology

Term	Definition
SHALL/MUST	This term is used to state a mandatory requirement of this policy
SHOULD	This term is used to state a recommended requirement of this policy
MAY	This term is used to state an optional requirement of this policy

4. Policy

This policy shall be used as a tool to inform Action for Children's employees, contractors and volunteers of their responsibilities to Action for Children so that they operate in a safe manner, continuously enabling the business to provide effective services to those in need.

4.1 General Use

4.1.1. Users must do their best to prevent unauthorised access to their devices, such as keeping them in secured access controlled areas during business and non-business hours. When devices are taken home, they shall be stored securely.

4.1.2. Action for Children users shall not leave their workstation unattended whilst connected to the Action for Children network. When leaving their desk, they shall either log off their session or lock the workstation.

4.1.3. When not in use all users shall ensure they have logged off and shut down their devices, this helps reduce the spread of viruses and malware.

4.1.4. Users shall not keep copies of any Action for Children account passwords, PINs, both door access and printer; this includes post-it's, in notebooks, diaries or stored on phones or laptops.

4.1.5. Users shall connect their device to the Action for Children network at least monthly to ensure they receive software patches and antivirus updates. Instructions on how to do this are available on Making IT Work.

4.2 Passwords

4.2.1 Passwords shall not be shared with anyone else.

4.2.2 Passwords shall fulfil the following requirements:

- Passwords to be 14 characters or more
- Passwords must contain 3 out of the following: lower case, upper case, number or special character.
- Passwords will expire after 1 year or less
- 12 previous passwords will be remembered so they cannot be reused
- Accounts will lock out if a password is entered incorrectly three times.

4.2.3 Passwords should be based on a passphrase.

4.2.4 Action for Children take guidance from The National Cyber Security Centre (NCSC) on strong password creation:

A good way to create a strong and memorable password is to use three random words. Numbers and symbols can still be used if needed, for example 3redhousemonkeys27!

A user should be creative and use words that are memorable to them, so that people can't guess the password. A user's social media accounts can give away vital clues about them. Users mustn't use words such as a child's name or favourite sports team which are easy for people to guess.

Cyber criminals are very smart and know many of the simple substitutions such as 'Pa55word!" which utilises symbols to replace letters.

Users must never use the following personal details for their password:

- Current partner's name
- Child's name
- Other family members' name
- Pet's name
- Place of birth
- Favourite holiday
- Something related to their favourite sports team

Users must not use the same password for multiple accounts and never write the passwords down.

4.3 Laptop & Tablet Protection

4.3.1 Action for Children laptop and tablet holders are responsible for the safety of the device and the data stored on it while in their possession.

4.3.2 Users shall ensure they follow device setup guidance so that corporate encryption solution is applied to the device.

4.3.3 In addition to the General Use terms set out in 4.1 above, due to the portability of laptops, users shall take reasonable extra measures to provide physical protection to it (i.e. a padded laptop case) when travelling or working in public places. Keep in mind the nature of the data on the device. Loss of a device could result in reputational damage and legal action towards Action for Children.

4.3.4 Users should also be aware of their surroundings and should not work on anything involving confidential or Action for Children group company sensitive data in a space where their screen may be visible to members of the public. If a user anticipates working in public spaces (eg cafe, train etc) on a frequent basis they should request a privacy screen from the Technology Department.

4.3.5 Computer workstations must be shut completely down at the end of the workday to protect data and install any security patches.

4.3.6 Laptops shall not be left unattended in public places.

4.3.7 Storing laptops or devices in a car is not encouraged, however if it is absolutely necessary a device shall be stored out of sight, e.g. in a locked car boot, for the shortest time possible.

4.4 Mobile Phones

This section covers mobile devices purchased, leased or loaned by Action for Children only.

4.4.1 Action for Children requires users to set a minimum 6-digit security pin on their phone or device. Biometrics (e.g. thumbprints) are approved on mobile phones (but not for other types of device).

4.4.2 Devices must be set up using the approved instructions provided by the Technology Department.

4.4.3 Mobile devices can be used to access corporate systems such as: Outlook, OneDrive, SharePoint and other corporate systems.

4.4.3.1 This is allowed on Action for Children group company managed mobile devices only and must be used in conjunction with InTune; the Action for Children approved Mobile Device Management solution.

4.4.4 Users shall only use apps that have been approved for corporate use and follow any guidance that has been issued for specific apps.

4.4.5 Users should set up a personalised voicemail message on their mobile phone indicating the message left will be heard by the intended person.

4.4.6 Users should ensure that their voice mail messages are cleared down regularly.

4.4.7 All removable media cards (eg SD cards) installed into mobile devices must have encryption enabled on them before any data is stored on them.

4.4.8 Users must not use their Action for Children SIM in a 3rd party phone or other device.

4.4.9 If user’s phone becomes lost, stolen or malfunctions they must contact the Technology Department as soon as possible and within 24 hours.

4.4.10 Users should consider the appropriateness of their location and the nature of the call they are on. Discussing sensitive information in a public area such as a train, coffee shop or a third-party office is not advisable.

4.4.10.1 This also includes the use of Teams/Skype and any other form of voice chat in public areas (as listed above).

4.4.11 Please refer to the WhatsApp policy for terms of use for this particular app.

4.4.12 For information on social media usage, please see the Social Media Policy.

4.5 Cameras

4.5.1 Where possible an AFC phone should be used to take photos as the storage is encrypted and photos can be securely transferred.

4.5.2 Cameras are only authorised for use as set out within the Cameras and Other Imaging Devices Policy.

4.5.3 Cameras and memory cards must be securely stored in a locked cupboard or filing cabinet in a locked office when not in use.

4.5.4 Any photos taken on the camera must be downloaded and deleted before the end of the working day.

4.5.5 Storing any other data on the camera's memory card is strictly forbidden.

4.5.6 Only cameras owned by Action for Children are authorised for use. Use of personal camera equipment within Action for Children services or whilst working for Action for Children is strictly forbidden.

4.5.7 Staff and volunteers must never use their own memory cards, storage, electronic or otherwise, to store or share images of service users.

4.6 Portable Media Devices

4.6.1 Action for Children's data must not be stored on portable media devices unless access is required when network connectivity is not available. Data should only be stored on authorised devices.

4.6.2 When a portable, Action for Children approved, data storage device is used, the instructions for the correct use must be followed to ensure the data is encrypted. The Technology Department maintain a register of approved data storage devices.

4.6.3 Personal storage media and equipment must not be connected to Action for Children's network and must not be used to store Action for Children's data.

4.6.4 Other portable USB devices include mobile phones, cameras, PDAs etc, must not be used to store Action for Children's data.

4.6.5 Only encrypted USB data storage devices issued by the Technology Department can be used to hold Action for Children's data.

4.6.6 The use of DVD/CD devices will be blocked by default, if there is a specific business requirement to use one of these devices a request should be made to the IT Service Desk with manager approval.

4.6.7 Where there is a need for a particular job function requiring write access to CD/DVD or floppy drives, this can be enabled as an exception and recorded formally with agreement from the IT Service Desk. Any agreement to allow write access to CD/DVD or floppy devices will include the conditional use of appropriate AES 128 / 256 bit encryption

4.6.8 Any other requirement for portable storage devices such as portable hard drives, magnetic/DAT tapes and devices must be escalated to the IT Service Desk and only hardware and software on Action for Children's approved software and hardware list is to be used.

4.6.9 Any and all passwords relating to portable devices must be handled with the utmost sensitivity / privacy and therefore must never be written down or stored in an unprotected format.

4.6.10 Action for Children employees, partner agencies, contractors and vendors undertaking work for Action for Children who are issued with portable storage devices to write, view, transmit, or access encrypted data, have a responsibility to ensure:

4.6.10.1 No one other than authorised person(s) are aware of the encryption/decryption password for the device, media or system

4.6.10.2 Any and all passwords relating to a portable device must be handled with the utmost sensitivity / privacy and therefore must never be written down or stored in an unprotected format.

4.6.10.3 Any portable device or media is not given to any unauthorised persons for safe keeping.

4.6.10.4 All reasonable steps must be taken to ensure that during transit, any portable device/media is locked via a key or combination lock and securely located. Portable devices/media must not be left unattended in any vehicle at any time due to insurance requirements.

4.6.10.5 Any portable device or media is adequately protected from physical damage.

4.6.10.6 Any portable device or media is not hired, lent out or given without authorisation from the IT Service Desk.

4.6.10.7 Any portable device or media which is no longer required or has reached its lifespan must be handed over to the IT Service Desk.

4.6.10.8 The device/media are handed back to the IT Service Desk on cessation of employment with Action for Children.

4.6.10.9 The device/media are handed back to the IT Service Desk when no longer authorised to use the device/media.

4.6.10.10 The loss of any portable device is notified immediately via Action for Children's Incident Reporting and Management Procedure.

4.6.11 The use of portable devices may be subject to random periodic review to ensure compliance with Action for Children's policies.

4.7 Clear Desk Policy

4.7.1 Users are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure at the end of the day and when they are expected to be away from their desk for an extended period.

4.7.2 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

4.7.3 Computer workstations must be locked when the workspace is unoccupied.

4.7.4 Filing cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

4.7.5 Keys used to access Restricted or Sensitive information must not be left at an unattended desk or unlocked location.

4.7.6 Laptops should not be left unattended for a prolonged time. Users should either take the laptop with them, lock it to a secure surface with a locking cable or lock it away in a drawer.

4.7.7 Whiteboards containing Restricted and/or Sensitive information should be erased after use.

4.7.8 Treat mass storage devices such as CDROM, DVD or other removable media as sensitive and secure them in a locked drawer.

4.8 Internet Acceptable Use

4.8.1 In order to ensure that Action for Children discharges its duty of care to its employees and customers and service users, it routinely logs user activity, including email, internet access, and corporate system access.

4.8.2 Action for Children's IT systems shall not be used to access, display, store, create, generate or send any material which may cause offence. Offensive material is determined by Action for Children on a case by case basis and may include sarcasm, poor language including swearing, or other inappropriate comments. Please see Action for Children HR policies on conduct for details.

4.8.3 Action for Children will consider 'offensive' any material which is pornographic, sexist, racist or abusive. Additionally, anything which contravenes the professional standards Action for Children seeks to maintain, which is illegal, or a breach of Action for Children policy and values.

4.8.4 Users are only permitted to carry out organisational activities using approved organisation devices and applications.

In addition, the following activity is not allowed:

4.8.5 Using non-authorised devices to connect to systems on the Action for Children network or to access cloud based applications, except in the case of accessing Action for Children's Virtual Desktop solution.

4.8.6 Using non-authorised devices or personal devices to take photos of children and young people.

4.8.7 Downloading of software and applications without the appropriate approval through Remedyforce and the Technology Approval Process.

4.8.8 Accessing gambling websites or sites that break UK laws. If a user has any queries as to what constitutes a gambling website, they should ask their manager.

4.8.8.1 Exceptions to this rule may be made for gambling sites as part of fundraising partnerships, users should ask their line manager for details if they have questions. Abusing any such exceptional privileges granted to, for example, gamble will remain in breach of this policy.

4.8.9 Any activity involved in preparation for acts of terrorism.

4.8.10 Sending unwarranted email (e.g. spam, phishing) that is in breach of Action for Children policies on fundraising and/or data protection.

4.8.11 Downloading, storing, using or transmitting material that may infringe copyright, trademark or other proprietary rights.

4.8.12 The impersonation of another Action for Children user or deliberate use of another user's account to access the internet and email services.

4.8.13 Undertaking deliberate activities that waste staff effort or network resources.

4.8.14 Introducing any form of computer virus or malware into the corporate network; in line with the Computer Misuse Act 1990.

4.8.15 Using Action for Children resources (including but not limited to) electricity, gas, water and internet to personally profit in any way, (including but not limited to) the generation of cryptocurrency or for running an alternative business venture.

4.8.16 Action for Children are subject to strict regulations governing the distribution of sensitive information to the public, the following activities are expressly forbidden:

4.8.16.1 Posting sensitive Action for Children information to message boards, mailing lists or news groups on the internet. This includes, but is not limited to financial, employee and service user information. Only data classified as "publicly available" can be shared.

4.8.16.2 Discussing confidential Action for Children related financial, employee and service user information in open chat rooms or discussion groups.

4.8.16.3 Disclosing information to the press or on social media unless explicitly approved by the Action for Children Media Team.

4.8.16.4 Users sharing their personal political views without authorisation when acting in their capacity as an employee, ambassador or representative of Action for Children.

4.8.17 The corporate video conferencing solution must be used for all internal meetings, this is currently Microsoft Teams. Users may join video conference meetings setup by 3rd party organisations, please see Knowledge Base Article 555 for a list of video conferencing solutions you are authorised to join. However, users must not setup meetings using such alternative platforms and must use the corporately provided solution.

4.8.18 Users must not connect their AFC laptop or mobile phone to any public wireless access point or router.

4.9 Data

4.9.1 Users shall not create or copy any databases onto the network without first consulting with the Technology Team.

4.9.2 Users shall not take copies of any group company data without prior permission of the Data Protection Officer and Data Owner.

4.9.3 Users should not use Action for Children data for purposes other than it was intended for. Personal use of Action for Children data is strictly prohibited.

4.9.4 Users shall only access corporate systems via the user interface provided for their use and shall not use any other tools to directly access them, unless approved in advance by the Technology Department.

4.9.5 Users shall not attempt to access information held on Action for Children's systems that they are not authorised to. If they are in doubt, they should ask their line manager.

4.9.6 Users must not use any Action for Children information for personal gain, for any purpose that is not related to the day to day running of Action for Children, or has not been specifically requested by a user's line manager.

4.9.7 Users must not give away or sell user / customer, colleague or any other corporate email lists, or other lists of large number of users for non-Action for Children business. If in doubt, they should ask their manager.

4.9.8 For further information, please see the Data Protection Policy.

4.10 Data Storage

4.10.1 Data that is to be shared with external parties must be uploaded to an approved SharePoint folder with appropriate permissions set. See the Sharing Appendix.

4.10.2 It is strongly recommended that files should be saved on OneDrive and SharePoint and not on legacy network drives.

4.10.3 At no time is a file or folder to be password protected for either internal or external use, as they cannot be scanned for malware, and stop our efforts to comply with access requests for GDPR and legal investigations.

4.10.4 Files should not be stored on the local hard disk of a device as this is not backed up.

4.10.5 The use of personal cloud services for the storage, processing or exchange of data relating to Action for Children is explicitly forbidden.

4.10.6 Please refer to the Sharing Appendix for further information.

4.11 Data Erasure

4.11.1 If a laptop or mobile device is lost or stolen it should be immediately reported to the Technology Service Desk.

4.11.2 The Technology department will then, where possible, execute either a factory reset of the device or remote wipe the data from the device. Where possible they will also block access to prevent the device being used.

4.11.3 If the device is stolen it should also be reported to the DPO and the Police, where relevant. In the event of a Police notification the Legal Team should be notified.

4.12 Printing

4.12.1 Where available secure printing shall always be used with a pin or login details being required to release the print job.

4.12.2 When printing, the document owner shall remain present and must collect all documents immediately.

4.12.3 When no longer required, all hard copies of Restricted and/or Sensitive documents shall be disposed of responsibly, where possible using a paper shredder or in the official shredder confidential waste bins.

4.13 Email Accounts

4.13.1 As with any Action for Children account, users must use the email account provided to them and must not allow anyone else to use it. Users are responsible for any actions taken or emails sent on their accounts.

4.13.2 Users should not access other user's email accounts without prior permission. Any access or attempted access to another user's email account shall result in disciplinary action.

4.13.3 Access to shared mailboxes shall be restricted to those necessary to achieve its purpose. If email accounts are to be shared, this should be done through the formal delegation process, not through the sharing of passwords.

4.13.4 Users are not permitted to auto-forward Action for Children mailboxes to personal or external email addresses.

4.13.5 Users shall not use an unapproved externally hosted email account such as Gmail or a personal Outlook account to represent Action for Children or to share or store resources.

4.14 Corporate Email

4.14.1 To avoid blacklisting with spam filters, complications to relationships and potential reputational damage, all emails being sent to multiple external recipients e.g. marketing emails, mail blasts and campaign promotions must be sent by the Action for Children approved mass mailing tool.

4.15 Sensitive Email

4.15.1 Emails containing sensitive information should be protected using appropriate encryption. Information on how to encrypt emails is included in the Technology knowledge base on Remedyforce here

4.15.2 Users should ensure the accuracy of their emails prior to sending. Users must remember to review the recipients and the content as it may be viewed by individuals other than for whom the message was intended.

4.16 Email Attachments

4.16.1 Attachments from unknown or untrusted sources must not be opened and users must not run or execute any programs, patches or scripts received via email.

4.16.2 Where possible users should not share files by attaching them to emails. Using a OneDrive link to share a document is the recommended method. Please see 3.21 Sharing Appendix.

4.17 Email Awareness

4.17.1 Users should remain vigilant at all times when opening and responding to emails. They should check that any email they receive is actually from who the sender claims to be. The malicious sender may use an alternative (but similar) email address or maybe able to “spoof” the real email address. For example, where the sender is asking for urgent payment, this should be verified with the sender via alternative means to check that it is genuine and not an impersonation attack.

4.18 Email Disclaimers

4.18.1 All external emails sent from the Action for Children must have an email disclaimer applied in order to make it clear that the organisation takes no responsibility for any loss or damage resulting from the recipient receiving, opening or using the email. It should also instruct the recipient of the email to immediately delete all copies of the email and any attachments should they receive the email in error.

4.19 Software Installation

4.19.1 If additional software is required, users must raise a ticket within Remedyforce which will be assessed by the Technology Department

4.19.2 Only preapproved apps can be installed on a user’s laptop or desktop device. Please see the Access Control Policy for further information.

4.19.3 Only preapproved apps can be installed by a user onto their mobile device. Please see the Access Control Policy for further information.

4.19.4 Staff, volunteers and/or contractors must not enter into contracts of any kind with cloud providers on behalf of Action for Children without first obtaining approval from the Technology Department.

4.20 Hardware Installation

4.20.1 If additional hardware is required, users shall raise a ticket within Remedyforce which will be assessed by the Technology Department.

4.20.2 Users shall not use hardware that has not been approved by the Technology Department.

4.20.3 All IT equipment must be purchased through the Technology Department. However, if a user already owns an existing peripheral eg a personal printer they are authorised to use this for work purposes, but no support can be provided.

4.20.4 Staff, Volunteers and Contractors must not modify any of Action for Children networks by installing any software or hardware devices such as routers, switches, hubs, wireless access points, Wifi boosters or any other device(s) without going through the formal Technology Department change process.

4.20.5 Users must not intentionally or otherwise bridge networks (be connected to the corporate and another network at the same time bridging the two networks). If a user does not understand this, they should raise a ticket in Remedyforce.

4.20.6 All best efforts must be made to always secure physical access to all IT equipment. In particular, networking devices should be secured by the use of measures such as CCTV, electronic locks, locked cabinets and any other security measures deemed appropriate.

4.21 Monitoring and Retention

4.21.1 All users of Action for Children services consent to all documents and communications, including email and internet access, remaining the property of Action for Children. Such documents and communications may be logged, retained and subject for review at any time by authorised Action for Children employees and third parties to ensure compliance with Action for Children's Security Policies.

4.22 Filtering

4.22.1 By using Action for Children's information systems, a user agrees to the monitoring of all their user activity for security and compliance purposes, including but not limited to files, web browsing and email.

4.22.2 Action for Children can choose to use tools to deny access to inappropriate sites, i.e. systems or websites that are not approved for business use.

4.22.3 Similarly filtering techniques can be used to ensure that inappropriate email is not sent from or received by Action for Children email accounts.

4.22.4 Where there are concerns about an employee/user's misuse of a system, Action for Children shall carry out the necessary investigations.

4.22.5 In order to gain access to monitoring or archived information for a direct report, a line manager must gain authorisation from their own line manager and provide this to the Technology Department.

4.23 Personal Use

4.23.1 Action for Children recognises that personal access to the internet at work helps employees to maintain a positive work life balance.

4.23.2 Limited and 'reasonable' personal use of internet access is permitted if it complies with Internet Acceptable Use 4.6.

4.23.3 Access to personal email accounts on corporate devices is prohibited as this poses a significant risk of data loss and breach of security.

4.23.4 Limited and 'reasonable' personal use of a work phone for calls and texts is permitted.

4.23.5 Personal use of all other systems is prohibited.

4.24 Remote Working

4.24.1 When working remotely users shall either use their Action for Children laptop or phone or connect to the Action for Children network via the approved AFC Virtual Desktop solution. Users should not attempt to access Action for Children systems or information resources via any other mechanism.

4.24.2 Users shall only login to the Action for Children network or an Action for Children device from within the UK, Guernsey and Ireland, unless prior permission has been granted by the IT Security Manager or their nominated delegate.

4.25 Training

4.25.1 It is mandatory for all users to complete the Information Security Essentials and Data Protection training and successfully pass the end of unit test within the first 6 months of employment and then to repeat the training and pass the test at least annually.

4.26 Breach of Policy

4.26.1 Action for Children users are expected to exercise good judgement and maintain a professional manner whenever using email or accessing the internet. Please be aware that breach of this policy may result in disciplinary action. Please see the Action for Children Disciplinary Policy for further information.

4.26.2 Criminal proceedings or Civil proceedings may also be actioned.

4.27 Sharing Appendix

4.27.1 Users shall comply with the Data Protection Act 2018, including ensuring that personal data is not shared with a 3rd party without obtaining the prior permission of the originating party or another lawful reason for processing that personal data in this way.

4.27.2 Business information should only be used for business purposes and in accordance with Action for Children's policies.

4.27.3 Emailing of files as attachments to external parties should be avoided where possible.

4.27.4 The use of any sharing sites including Dropbox and Google Drive is forbidden unless an authorised business case has been approved by the Technology Department.

4.27.5 Action for Children have approved secure methods for sharing information with 3rd parties; these methods protect the confidentiality and integrity of our data and make sure the organisation stays in control of its data for regulation compliance and security.

4.27.6 To share data with external parties, such as other businesses or contractors, users should make use of external SharePoint sites as a collaboration space.

- If a user would like to use this feature they must submit a ticket via Remedyforce; this will be reviewed by the Change Advisory Board.
- The case is then assessed on the perceived business need and security implications of sharing the data.
- Acceptance is not guaranteed, but the Technology Department will work with the user to find a solution that best fits Action for Children and their requirements.

4.27.7 The use of WeTransfer may also be used by departments where approved by the Technology Department and the category of data is not confidential.

4.27.8 It is the responsibility of the end user to only share video with appropriate individuals. This includes pre-recorded videos, video conferencing (e.g. via Skype for Business or Microsoft Teams) or via any form of screen sharing technology.

5. Relevant Policies

For additional information please see the following policies:

- Data Protection Policy and Procedure

- Social Media Policy
- WhatsApp Policy

6. Glossary of Terms

Non-authorised device - Any device which is not been specifically approved and supplied by the Action for Children Technology department. Examples of this include (but are not limited to) devices purchased by users directly from a supplier, personal devices or devices provided by a local authority.