HOW ACTION FOR CHILDREN WORKS

Service User ICT

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 are committed to the safeguarding of children and young people, staff, volunteers.

Policy Name:	Service User ICT
Document Name:	Service User ICT Procedures
Document Type:	Procedure
Policy Area:	Children's Services
Owner:	Practice Improvement
Approved by:	Director of Practice Improvement
Current Contact:	Head of Safeguarding
Date Issued / Last Updated:	21 February 2020
Latest Date to be re-updated and reapproved:	21 February 2021

Service User ICT Procedures

Contents

Advice and information on internet safety

The guidance to this procedure has information about places to find up to date information about internet safety. These are suitable for either staff seeking advice for their Service or for staff advising service users and/or parents/carers.

Notes

- Services which are part of the InspireIT project use the procedures and forms put in place as part of that project

Procedures

1. Service arrangements

Service ICT and Internet Access Policy

1.1. Service Managers (or delegated staff members) are responsible for producing the policy.

1.2. The policy is produced with the participation of children and young people, adults who are service users and, where appropriate, parents/carers.

1.3. The policy includes the following – where those coloured green are optional:

Statement of why this policy is required

Service issues

What the benefits are to service users and the Service – *i.e. the desired outcome of ICT use*

How ICT use will provide effective learning and personal development for service users

How service staff and service users will be consulted in developing the policy

Extent of access to be provided

Whether there will be access to e-mail, if so why and how will this be managed

What other Internet applications or services will be made available – e.g. access to social media services

Local procedures

How the risks will be assessed and safety assured

How safe, appropriate and lawful conduct will be taught, discussed and signed up to by way of an Acceptable ICT Use Agreement i.e. what the rules are.

How health and safety with computers will be maintained

How security will be maintained and supervision will be undertaken

How parents/carers support and permission will be sought for their child to access the Internet/use other equipment

How often the service policy will be reviewed

How the monitoring of Internet/equipment use will be undertaken – including service users own equipment used within the Service

How other technology may or may not be used i.e. mobile phones with integral cameras, digital cameras, Web cams, CD copiers, scanners etc. – *only appropriate where these will be in use*

The use of service users' own equipment within the service – including:

Whether all or some or no users will be given access to the Service DEA Wi-Fi

What monitoring and/or parental controls will be required on the equipment before it can be used

How it will be monitored

Whether service users can use their own mobile internet access on Service premises or at Service activities – *for adult users a ban on this is likely to be ineffective however the same condition around accessing inappropriate content can be applied*

Where within the premises it can be used – only appropriate where there is an assessed risk in any use in any particular area of the Service

The use of cameras and other imaging devices by service users in the service including controls and sanctions – see *Cameras and imaging devices in Services Policy*

What sanctions will be used if the Acceptable ICT Use Agreement is broken by a service user – *Services should refer to the Behaviour Support Policy* for advice on sanctions

How complaints will be handled

Training provision

How service users will be taught to use a PC and access the Internet

How intellectual property rights/copyright will be respected – *i.e. that service users do not download or share material that they have no right to download or share.*

The types of sites that children and young people can access and how this is monitored

1.4. The policy is reviewed at least annually. The review process includes:

- Taking account of changes to the service and changes in technology
- Assessing the benefits to service users of the ICT equipment and services
- Assessing whether it contributes to the outcomes for service users

1.5. If the review finds that ICT related activities are not actively contributing to the Service or Service User Outcomes, Staff may consider whether to continue to provide the present services, modify those services or discontinue them.

'Service user friendly' Local Policy

1.6. After an agreed Local Policy is produced Services produce a version for service users – more than one version may be required dependent on the range of service users. This contains as a minimum:

- The use or uses of any ICT services or equipment supplied by the Service
- The use or uses of any ICT services or equipment bought into the Service by individual service users
- Prohibited uses of the ICT services or equipment
- Sanctions that may be applied for misuse
- Processes for gaining access – e.g. booking time on a shared PC or applying for a mobile phone to be supplied
- How to report:
    - Misuse
    - Accidental accessing of inappropriate contact
    - Inappropriate approaches while using Action for Children ICT
    - Bullying

1.7. Reviews of the Local Policy may require revision of the 'service user friendly' version.

Equipment and internet access

Internet access

NOTE: Services may use the DEA public use internet access for service user use; however, this may not be sufficient for heavy service user use or activities that include use of media such as video. Services can seek advice from IS on whether they need to install additional internet access.

1.8. Where Services have additional internet access installed, they ensure that the internet access/feed is filtered for adult content or able to be configured to filter adult content – where this is not possible see equipment below.

1.9. Services will need to address the issue of service users using their own mobile internet access within Services in the Local Policy. Service users using their own mobile internet access in Services or during Service, activities must not access material that is inappropriate.

Suitable equipment and services

1.10. Service Managers ensure that all ICT equipment and services obtained for service users are able to be configured to meet the needs of this policy and any conditions laid down for individual service users in their Acceptable Use Agreement.

1.11. Where desk or laptop computers or tablets are to be provided Service Managers ensure that appropriate filtering and/or parental control software is installed and this will be recorded on the equipment inventory.

1.12. Service Managers ensure that filtering and/or parental control software is configured to reflect the access conditions set in the Acceptable Use Agreement for individual service users.

1.13. Where mobile phones are provided to service users Service Managers will ensure that any internet access possible using the device is configurable. Service Managers ensure that this is configured to reflect the access conditions set in the Acceptable Use Agreement for individual service users

1.14. Any games – either accessed via the internet or on disk – should be suitable for service users allowed to use them. Staff assessing this use both any Rating and age limits on the game and an assessment of the content for appropriateness.

Donated equipment

1.15. Service Managers ensure that equipment donated to services can be configured to meet the needs of this policy.

1.16. If equipment is being donated by a company – for example where it has adaptive technologies installed or included that they produce – services request that it is preconfigured to meet the needs of this policy.

1.17. If it cannot be configured to meet the needs of this policy, use of the equipment should not be ruled out. For example it could be used unconnected to the internet.

Access to ICT equipment

1.18. Service Managers ensure that staff are aware that ICT equipment available for the use of service users is not to be used for business use.

1.19. Service Managers and staff ensure that service users do not use business ICT equipment.

Equipment inventories

1.20. Service Managers maintain inventories of ICT equipment purchased for the use of service users. This includes:

- Date of purchase
- Dates of any maintenance on the equipment
- Whether it was purchased for communal use or individual use
- If purchased for individual use the details of the individual service user and the person responsible for the safekeeping of the equipment

2. Safe and appropriate use of ICT

Health & Safety

2.1. A Health and Safety Assessment of the equipment and its location or proposed location is undertaken (See Health & Safety Manual).

2.2. If the equipment is for use outside the Service, service users and parents/carers are provided with appropriate advice and information on siting the equipment and use

Inappropriate material

2.3. No sites or services containing

- Child pornography
- Content that is criminally obscene
- Adult material of a sexual nature

- Content that incites racial hatred or belief hatred
- Content that does not 'fit' with the organisation's Equality and Diversity principles

Must be accessed using Action for Children provided internet access or equipment.

2.4. In addition to the above Services may decide to filter other sites or services dependent on their service users.

ICT equipment and services within services

2.5. Service users using the equipment and services must be aware of the service procedure for reporting concerns such as inappropriate contact by adults or others, or inadvertent access to inappropriate material, and should be encouraged to do so.

2.6. Wherever possible equipment is sited in a location where staff are able to supervise its use.

2.7. Service users will have individual user accounts with user names and passwords on any computers available for group access, unless the computer is for drop-in use.

2.8. Where necessary parental control software is installed and configured appropriately. This software can be configured to restrict access to websites and restrict the use of certain software – for example chat or instant messaging.

2.9. Staff regularly monitor:

- Internet sites visited
- Whether unauthorised software has been used
- For the use of age inappropriate services or sites

2.10. If the monitoring of shared equipment shows that users are breaking the Acceptable Use Agreement proportionate sanctions are applied after investigation – *See Behaviour Support Policy.*

The use of cameras and other imaging devices in Services or during Service activities

See *Cameras and other imaging devices within Services Policy* – which includes service users taking images.

ICT equipment and services for the sole use of individual service users

2.11. Service users using the equipment and services must be aware of the service procedure for reporting concerns such as inappropriate contact by adults or others, or inadvertent access of inappropriate material, and should be encouraged to do so.

2.12. Staff and/or the person with parental responsibility monitor use regularly to ensure that the conditions of access are being adhered to.

2.13. Staff and/or the person with parental responsibility monitor for use of age inappropriate services or sites – some sites have age limits for registering. Any inappropriate use should be addressed.

2.14. If service users refuse to allow monitoring staff, consider applying a sanction. This could include restricting the use of equipment to service premises or with service staff or the removal of services.

2.15. Sanctions applied must be proportionate and must not create other risks for the individual – for example, removal of access to a PC may result in the inability of the service user to complete homework.

Meeting life skills and curriculum needs

2.16. Staff, foster carers and prospective adopters encourage the use of the internet to help children and young people develop living skills and to meet their educational needs.

Social networking

2.17. Part of the risk assessment carried out includes an assessment of whether service users can be allowed access to social networking services; this includes any safeguarding and legal issues – for example Court Orders being in place on a child or young person.

2.18. Before allowing service users access to social networking sites staff ensure that:

- the child or young person is aware of the risks involved in the use of such sites:
    - inappropriate approaches by people unknown or known to the child or young person
    - inappropriate posting of materials
    - bullying
- they have reviewed the available privacy setting available on the sites and agreed a setting to be used
- discussed and agreed what the child or young person should do if contacted inappropriately or if they have inappropriate content posted to their page (note that Facebook allows for a setting to disallow photos 'tagged' with a users name by other Facebook users to be shown in their photo stream)

2.19. If a service user is using a social networking service that is inappropriate (e.g. they are too young or old) contact the site and ask for their account to be removed. If this is unsuccessful, contact the Head of Safeguarding who will take further action.

Service user generated content

2.20. Staff ensure that they are aware of any content that is being generated by individuals or groups of service users.

2.21. Material produced using Action for Children ICT is not published without being approved.

2.22. Any material produced by groups using Action for Children ICT for external publication meets our general acceptability requirements – i.e. material produced by service users should not be such that we would not allow access to it. Additionally:

- Note the procedure around the use of cameras in services
- Note and action any legal restrictions – for example Court Orders - that may apply to any service users – for example certain children and young people may not have their image published
- Note the requirements for positive images of our activities

If staff are uncertain then they should seek advice.

3. ICT Services for groups (children, young people and adults)

3.1. When considering the provision of ICT within services staff must carry out a risk assessment. This risk assessment must include consideration of:

- Benefits that use might give to service users
- The services that the equipment will be used for
- Any individual service users that may be at a higher risk
- Any skills gaps in the staff group
- If internet access is under consideration then the risk assessment must include possible use of social networking services.

3.2. Where an individual service user is at a higher risk they must be risk assessed individually. This risk assessment will inform their Acceptable ICT Use Agreement. An example risk assessment can be found in the Forms that are part of this policy.

The risk assessment will include the participation of:

- The service user
- Parents/carers or person with parental responsibility if appropriate

If internet access is under consideration then the risk assessment must include possible use of social networking services.

If the risk assessment results in the refusal of service this must be communicated to the service user and parents/carers or person with parental responsibility.

3.3. If it is decided that ICT services will be provided within the service then:

- Appropriate permissions for all service users who are going to use the ICT equipment must be obtained Form 3 - Acceptable use agreement.

  Parental consent. Young people aged 16 and over in Scotland are able to sign in their own right and do not need the signature of a parent/carer or person with parental responsibility, if appropriate.
- All service users must have individual Acceptable ICT Use Agreements
- All service users must be given basic training and made aware of Action for Children NetSmart Rules

3.4. Service staff ensure that service users understand the risks and benefits of internet use.

4. ICT equipment for drop-in use (children, young people and adults)

4.1. Where equipment is provided on a drop-in basis for the use of service users:

- Computers must be equipped with filtering software
- The acceptable use rules must be displayed in the room where the computers are located
- Individual log-ins are not required but all service users must sign a log and their start and end times must be recorded

4.2. Where drop-in users include children and young people the service must be supervised.

5. Access to Action for Children ICT for individuals (children and young people)

NOTE: This section applies when a Service is supplying a service or equipment to be used by one particular service user in or outside of the Service.

5.1. When a request is made by the parents/carers or person with parental responsibility for ICT services they must be sent a copy of the Service ICT and Internet Access Policy

5.2. When considering giving children or young people access to Action for Children ICT, a risk assessment of the individual service user must be made. An example risk assessment can be found in the Forms that are part of this policy.

5.3. The risk assessment will include the participation of:

- The service user
- Parents/carers or person with parental responsibility if appropriate

5.4. If internet access is under consideration then the risk assessment must include possible use of social networking services.

5.5. If the risk assessment results in the refusal of service this must be communicated to the service user and parents/carers or person with parental responsibility.

5.6. If service provision is agreed:

- Obtain written permission from the parents/carers or person with parental responsibility using Form3 - Acceptable use agreement:

  Parental consent Young people aged 16 and over in Scotland are able to sign in their own right and do not need the signature of a parent/carer or person with parental responsibility.
- Ensure that the parents/carers or person with parental responsibility understands that any equipment provided remains the property of Action for Children and it must be returned when requested
- Ensure that the service user understands any conditions of use set taking the risk assessment and views of the service user and parents/carers or person with parental responsibility into account. This may include:
  - Monitoring requirements
  - Limitations in use
- The service user must sign the Acceptable ICT Use Agreement (Form 3 - Acceptable Use Agreement) which will include a statement of their conditions of use

5.7. If the agreed service provision includes use of Action for Children ICT outside of Action for Children services; a person with parental responsibility must sign the form (Form 4 - Maintenance and Settings Agreement) to accept responsibility for the maintenance of the machine and the loaded controls set for the individual service user on the machine.

Young people aged 16 and over in Scotland are able to sign in their own right and do not need the signature of a parent/carer or person with parental responsibility.

5.8. When signing the Acceptable Use Agreement service users must be provided with the Action for Children NetSmart Rules.

5.9. Service staff ensure that service users understand the risks and benefits in internet use.

Mobile phones

5.10. The procedures (see 2.5 to 2.11) as regards risk assessment and the various permissions must be followed if mobile phones are to be provided to individuals.

5.11. It must be agreed what the general use of the supplied mobile is.

5.12. Individual service users and parents/carers/person with parental responsibility must be made aware of the risks of using mobiles inappropriately.

Provision of equipment

5.13. Before equipment is provided the service user or service users who are going to use it must be:

- Made aware of the service procedures for reporting concerns
- Told how they are to be supervised and/or monitored
- Be given some basic tuition on the use of the equipment

5.14. A designated staff member must ensure that any filtering or parental control software is configured.

6. Service users using their own equipment (children, young people and adults)

NOTE: Children and young people may bring their own equipment into our services – especially Family Placement, Residential and Schools – but there are requirements for their use. Services where service users will not be there 24 hours a day may find it easier to substantially restrict this equipment use

6.1. Where service users bring their own equipment for use inside Services staff should apply the same procedure as for individual service users above.

6.2. Before being used within the Service computers have appropriate monitoring and parental control software installed (as for Service equipment). Refusal to allow this software to be installed leads to use being disallowed.

6.3. Service staff monitor use of the equipment as for any Service equipment

Adult service users

6.4. **Using their own computers and Action for Children internet access** – we do not require monitoring but a Form 2 – Acceptable Use Agreement must be signed. Service users will be allowed access as they wish – unless their circumstances dictate that some restrictions are required.

6.5. **Using their computers and their own internet access** – services ensure that service users have been given advice and support on internet use.

7. Use of other interactive services

7.1. Service users and, where appropriate, parents/carers/persons with parental responsibility are made aware of the risks of the using other interactive services that might be accessible using Action for Children supplied equipment e.g.:

- Text to television services that allow messages and/or pictures to be uploaded using a mobile phone
- Email to television services that allow messages to be emailed in

7.2. Where service users might be found to be putting themselves at risk by using these services appropriate action should be taken. For example if a service user is uploading inappropriate pictures via their mobile phone's camera an alternative camera-less phone might be provided instead.

8. Reporting Concerns

NOTE: Where incidents of concern are considered to be significant – this includes, but is not limited to, any incident where reports are made to any outside organisation/service - Service/Service Managers follow the Reputational Risk Management Policy procedure

Inappropriate contact/grooming

8.1. Any inappropriate contact – whether this is found by monitoring or reported to you by the service user - is reported to the police and/or to the Child Exploitation and Online Protection Centre (http://www.ceop.gov.uk). See Guidance for further information on who you should report this to. Ensure that you inform the police that you have reported it to CEOP and CEOP the police.

8.2. Any contact from someone who is a known risk to a particular service user is reported to the police.

Email containing material relating to the viewing or downloading of child pornography

8.3. The supervising adult will forward these directly to the Internet Watch Foundation following the instructions on their website (http://iwf.org.uk)

Websites containing child pornography, content that is criminally obscene or content that incites to racial hatred

8.4. If sites containing this content are inadvertently accessed using Action for Children ICT equipment forward details of the site to the Internet Watch Foundation.

Inappropriate content on social networking sites

8.5. Material that is posted by other users can usually be removed through use of the 'Report this' function on many sites. If you are unable to do this, contact the Head of Safeguarding.

8.6. Material that is posted by the service user can usually be removed via their own account. If not, contact the site itself to ask for it to be removed. If you are unable to do this, contact the Head of Safeguarding.

Abusive or bullying emails or text messages

8.7. If a child or young person receives abusive or bullying emails report this to the senders email provider – you can work this out from the text after the @ symbol e.g.

if the originating email address is jo.smith@googlemail.com then the email provider is google mail. Most email providers will provide an address to report email abuse to.

8.8. For abusive or bullying texts, you may address this in different ways depending on whether you know who is sending them or not. For example if it is a school pupil known to the child or young person, you may address this through the school. If it is from an unknown source, report it to the mobile provider.

8.9. Dependent on the seriousness of the abusive emails or texts you may feel that contacting the police is appropriate. Abusive emails can be reported to CEOP.

Interactive television services

8.10. If you have any concerns about interactive television services contact Ofcom (www.ofcom.org.uk)

Mobile phone services

8.11. Complaints or concerns about mobile phone operators contact Ofcom (www.ofcom.org.uk)

8.12. Complaints or concerns about mobile phone services contact PhonepayPlus (http://www.phonepayplus.org.uk/)

Inappropriate or illegal materials found on or suspected to be on service user ICT equipment

8.13. Where inappropriate or illegal material is found on, or suspected to be on, service ICT equipment staff follow the Equipment Examination Procedure that is part of the Managing allegations and safeguarding concerns regarding staff, volunteers and carers procedure within the Safeguarding Framework.

8.14. Guidance on what inappropriate or illegal material is in the Equipment Examination Procedure but additionally includes evidence or suspected evidence of inappropriate contact/grooming or inappropriate emails.

8.15. Inappropriate or illegal materials found on or suspected to be on service user ICT equipment will not require reporting to the designated local authority offer unless it is suspected or known that a staff member has some involvement in the incident.

8.16. Service/Service Managers follow the Reputational Risk Management Policy procedure where inappropriate or illegal material is found on, or suspected to be on, service user ICT equipment.