Internet Safety Policy

Author	Lorna Lightfoot
Reviewed	March 2019
Version	1
Approved	March 2019
Cross Reference	UK Safer Internet Centre (www.saferinternet.org.uk), wwww.childline.org.uk, www.getconnected.org.uk, www.thinkuknow.co.uk, www.nspcc.org.uk/onlinesafety, www.childnet.com, www.ceop-police.uk/safety-centre, General Data Protection Regulation (GDPR) 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, 2016 (RIPA) and the Lawful Business Practice Regulations 2000
Next Review Date	2021

Purpose of this document

Computing covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole. Currently the internet technologies children and young people are using include:

- Websites
- E mail and Instant Messaging
- Chat rooms (including live streaming) and social networking
- Blogs and Twitter
- Podcasting
- Video broadcasting
- File sharing (both uploading and downloading files)
- Gaming
- Mobile / smart phones with text, video and / or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, most of the above, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Aspired Futures we understand the responsibility to educate our children and young people (CYP), staff and volunteers on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

POLICIES AND PROCEDURES

Aspired Futures holds personal data on children, young people, volunteers, staff and others to help us conduct our day-to-day activities. Everybody at Aspired Futures has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all children, young people, volunteers, staff and trustees) are inclusive of both fixed and mobile internet; technologies provided by Aspired Futures and technologies owned by children, young people, staff or volunteers bought onto the charity's premises.

Monitoring

Any member of the Senior Management Team (SMT) may inspect any computing equipment owned or leased by Aspired Futures at any time without prior notice.

SMT may monitor, access, inspect, record and disclose telephone calls, e-mails, internet use and any other electronic communication (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain Aspired Futures business related information; to confirm or investigate compliance with our policies, standards and procedures; to ensure the effective operation of Aspired Futures ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1988, or to prevent or detect crime.

All monitoring, surveillance or investigative activities are conducted by authorised staff or their representatives and comply with the GDPR 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Breaches

A breach or suspect breach of policy by an Aspired Futures employee, contractor, volunteer or CYP may result in the temporary or permanent withdrawal of access to the internet whilst on Aspired Futures premises.

Any policy breach is grounds for disciplinary action in accordance with our Disciplinary procedure

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Services and Volunteer Manager or another member of SMT.

Staff

Aspired Futures

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;

- Makes regular training available to staff on e-safety issues
- Provides, as part of the induction process, all new staff (including those on student placement) with information and guidance on the e-safety policy and the charity's Acceptable Use Agreements.

Parents / Carers

Aspired Futures provides

- Introduction of the Acceptable Use Agreements to all parents / carers, to ensure that principles of e-safe behaviour are made clear.
- Suggestions for safe internet use at home (where appropriate)
- Provision of information about national support sites for parents

Children and Young People

Aspired Futures

- CYP to STOP and THINK before they CLICK
- the SMART rules (Safe, Meeting, Accepting, Reliable, Tell)
- to understand acceptable behaviour when using an online environment / e mail, ie to be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why online "friends" may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have appropriate privacy settings turned on
- To understand why they must not post pictures or videos of others without permission
- To know not to download any files without permission
- To have strategies for dealing with inappropriate material
- To understand the impact of cyberbullying, sexting, trolling and know how to seek help if they experience problems when using the internet and related technologies, ie parent or carer, trusted staff member, or organisations such as Childline

Plans internet use carefully to ensure that it is age appropriate and supports the objectives for specific tasks or projects

- Will remind CYP about their responsibilities through an End-User Acceptable Use Agreement which every CYP will be asked to sign and which will be displayed on noticeboards throughout the building
- Ensures staff will model safe and responsible behaviour in their own use of technology during sessions
- Ensures that when copying materials from the web, staff, volunteers and CYP understand issues around plagiarism and how they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff, volunteers and CYP understand the issues around aspects of commercial use of the internet as age appropriate. This may include risks in pop-up adverts, gaming online, gambling etc;

POLICIES AND PROCEDURES

Aspired Futures E-Safety Rules

Children and Young People Acceptable Use Agreement

These rules reflect the content of our Internet Safety Policy, it is important that parents / carers read and discuss the following statements with their child, understanding and agreeing to follow Aspired Futures' rules on using ICT, including use of the internet.

1. I will only use ICT at Aspired Futures for approved projects
2. I must obtain prior approval from a member of Aspired Futures SMT if I wish to bring personal IT equipment onto Aspired Futures premises. Phones will be turned off and stored securely during sessions (please refer to Appendix 1)
3. I will only use the internet and / or online tools responsibly
4. I will not deliberately look for, save or send anything that could be unpleasant or nasty
5. If I accidentally find anything inappropriate, I will tell a member of the Aspired Futures team immediately
6. I will not deliberately bring in inappropriate electronic materials from home
7. I will not look at or deliberately access inappropriate websites
8. I will make sure that all ICT related contact with others is responsible, sensible and polite
9. I will not give personal details out online, either for myself or other people
10. I will only open, edit or delete my own files
11. I will not attempt to download or install files without permission from a member of the Aspired Futures team
12. I will use ICT responsibly; I know the rules in place are there to keep me safe
13. I know that my use of ICT can be monitored, and my parents / carer will be contacted if Aspired Futures have any concerns about my safety online.
14. I will only use ICT equipment at Aspired Futures when accompanied by a member of staff or a volunteer.

We have discussed this Acceptable Use Agreement and

…….(print child's name) agrees to follow the Internet Safety rules and to support the safe use of ICT at Aspired Futures.

Parent / carer Name (Please print)……..

Parent / carer signature…… Date……

This AUA must be signed and returned to Aspired Futures before any access to the internet during sessions will be permitted.

POLICIES AND PROCEDURES

Appendix 1

The use of mobile phones and other personal devices by CYP at Aspired Futures will be decided by Aspired Futures staff and covered by this policy. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the charity and any breaches will be dealt with as part of the discipline / behaviour policy. Aspired Futures staff may confiscate any device if they believe it is being used to contravene any part of the policy. The phone or device may be searched by a member of SMT with the consent of the CYP and / or parent / carer. If there is a suspicion that the material on the device may provide evidence relating to a criminal offence the device will be handed over to the police.

Mobile phones should be switched off at all times whilst at Aspired Futures

Electronic devices which are bought into Aspired Futures are the responsibility of the user. Aspired Futures accepts no responsibility for the loss, theft or damage of such items. Nor will the charity accept responsibility for any adverse health effects caused by any such devices either actual or potential.

CYP use of personal devices

- If a CYP breaches the charity's policy, the device will be confiscated and held in a secure location in the small office. Mobile phones and devices will be released to parents / carers on accordance with this policy.
- If CYP need to contact parents/ carers during sessions or outings, they can use the office phone or a staff work mobile phone. Any mobile phone belonging to CYP will be turned off during sessions and will be stored in a secure location. If parents / carers need to speak to CYP during a session, they should use the office phone.
- CYP should only give their personal mobile phone numbers out to trusted individuals.

POLICIES AND PROCEDURES

ICT Acceptable Use Agreement (AUA)

Staff, Volunteers, Trustees and Visitors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff, volunteers, trustees and visitors are aware of their individual responsibilities when using technology. All staff members, volunteers, trustees and visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head of Services.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in eSafety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether provided by Aspired Futures or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside of the workplace that may bring the charity, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms. (See Appendix 1)
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will adhere to the staff personal device policy e.g. mobile phones and tablets. (Appendix 2)
9. I will not install any hardware or software without the prior permission of SMT or their designated representative.
10. I will ensure that personal data is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with charity policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the charity's network without the prior permission of the parent/carer, or person/s in the image.
12. I will report any known misuses of technology, including the unacceptable behaviours of others.
13. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
14. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

15. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
16. I understand that network activities and online communications may be monitored, including any personal and private communications made using Aspired Futures systems.
17. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
18. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the charity's Internet Safety policy and help children to be safe and responsible in their use of ICT and related technologies.
19. I understand that these rules are designed for the safety of all users and that if they are not followed, sanctions will be applied and disciplinary action taken.

I have read and agree to follow this code of conduct and to support the safe use of ICT.

Signature ……

Date ……

Full Name …… (PRINT)

Position/Role ……

Appendix 1

Staff will ensure that in private use:

- No reference should be made in social media to pupils, parents / carers, volunteers or staff.
- They do not engage in online discussion on personal matters relating to members of the Aspired Futures community.
- Personal opinions should not be attributed to the charity.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Appendix 2

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a work phone where contact with CYP or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during sessions or outings

unless permission has been given by a member of SMT in emergency circumstances. (If needing to make a personal phone call the member of staff needs to ask for session cover.)

- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the SMT.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches this policy then disciplinary action may be taken.
- Staff must use the dedicated team e mail address when corresponding with CYP

ICT Acceptable Use Agreement (AUA) Parents and Carers

ICT and the related technologies such as e-mail, the Internet (Social Networking Sites) and mobile devices are an integral part of our daily life. This agreement is designed to ensure that all parents and carers are aware of their individual responsibilities when using technology. All parents and carers are asked to sign this policy and adhere to it at all times. By working together we hope to develop the children's awareness and understanding of how to be safe and happy while using developing technologies. Any concerns or clarification should be discussed with the Head of Service.

Rules and Guidance
Parent's and carers:

1. Will support the charity's approach to on-line safety and not deliberately upload or add any images, sounds or text (Online discussions) that could upset or offend any members of the charity.
2. Should provide consent for CYP to use the Internet, as well as other technologies, as part of the e-safety Acceptable Use Agreement form at the time of their child's entry to the charity and review it on a regular basis.
3. Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse as per the Internet Safety policy.
4. Parents / carers are specifically informed of e-safety incidents involving their child and given support where needed.
5. Support the charity in promoting e-safety and endorse the Parents' Acceptable Use agreement which includes the CYP's use of the Internet and the charity's use of photographic and video images.
6. Will read, understand and promote the charity's Pupil Acceptable Use Agreement with their children.
7. To consult with Aspired Futures if they have any concerns about their children's use of technology, including any restrictions to internet use.

We will seek advice from outside agencies if one of our CYP's parents / carers or staff receives communication that we consider is particularly disturbing or breaches our policy.

I have read and agree to follow this code of conduct and to support the safe use of ICT.

Childs Name……

Signature ……

Full Name …… (PRINT) Date ……

Aspired Futures ICT Infrastructure

E-mail

Aspired Futures

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of CYP or staff on the charity's website. We use a group e-mail address.
- Will contact the Police if one of our staff, volunteers or CYP receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems, including desktop anti-virus products, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language

CYP

- CYP cannot receive external email

- CYP are taught about the safety and 'netiquette' of using e-mail i.e. they are taught:

  O Not to give out their e-mail address unless it is part of a managed project or to someone they know and trust and is approved by an Aspired Futures team member or parent/carer;

  O That an e-mail is a form of publishing where the message should be clear, short and concise;

  O They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;

  O To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;

  O That they should think carefully before sending any attachments;

  O Embedding adverts is not allowed;

  O Not to arrange to meet anyone they meet through e-mail

  CYP sign the school Acceptable Use Agreement Form to say they have read and understood the Internet safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Never use email to transfer staff or CYP personal data to volunteers or visitors and only transfer appropriate information to approved members of staff.

- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on headed paper. That it should follow the 'house-style':

- The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;

- All staff sign our Acceptable Use Agreement Form AUA to say they have read and understood the internet safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

POLICIES AND PROCEDURES

Aspired Futures Website

- The Head of Business takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: <e.g. Head of Business or SMR Manager >
- The point of contact on the web site is the charity address, telephone number and we use a general email contact address;
- Photographs published on the web do not have full names attached;
- We do not use CYP's names when saving images in the file names or in the tags when publishing to the charity's website.

Social networking

All stakeholders follow the charity's Acceptable Use Agreements with regard to social networking.

Data security: Management Information System access and Data transfer

Strategic and operational practices

At Aspired Futures:

- The Head of Service is the Designated Safeguarding Lead / Prevent Lead
- We ensure staff know to report any incidents where data protection may have been compromised to the Designated Safeguarding Lead / Prevent Lead.
- All staff are DBS checked and records are held in one central record.
- We ensure ALL the following stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

- staff,
- trustees,
- CYP
- parents / carers

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the office and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.

- Staff with access to setting-up usernames and passwords for email and network access are working within the approved system and follow the security processes required by those systems.

- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have a secure area on the network to store sensitive data and photographs

- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after computers are idle for 15 minutes.

- Any sensitive information taken off site is by authorised personnel only.

- We store any sensitive written material in lockable storage cabinets in a lockable storage area.

- All servers are in lockable locations and managed by DBS-checked staff.

- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.

- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.

- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.

POLICIES AND PROCEDURES