

E-safety Policy



Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

A planned e-safety curriculum should be provided as part of PHSE and should be regularly revisited. Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities. Staff should act as good role models in their use of digital technologies the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the relevant designated person can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education & Training – Staff/Volunteers:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The Designated Senior Person (or other nominated person) will receive regular updates through attendance at external training events/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings.
- The E-Safety Coordinator will provide advice/guidance/training to individuals as required.

Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers (email, chat, etc) must be professional in tone and content.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school/ website and only official email addresses should be used to identify members of staff.

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information: Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues. Clear reporting guidance, including responsibilities, procedures and sanctions. Risk assessment, including legal risk. School staff should ensure that: No reference should be made in social media to students, parents/carers or school staff. They do not engage in online discussion on personal matters relating to members of the school community. Personal opinions should not be attributed to the school or local authority

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. This also includes the deliberate searching for inappropriate materials and the consequences for doing so. This can be shown by signing the Induction Booklet so that it is clear to the school/education setting or other establishment that the agreement are accepted by the child or young person.

Version 1

To be updated July 2017

Signed Manager

M. Martin

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur: Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity. Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time. A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult. In the event that a child or young person accidentally accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment. Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Acceptable User Agreement – Staff Members



New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure: that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use, that staff are protected from potential risk in their use of ICT in their everyday work. Action Learning will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users. This policy applies to any device in school. This means that when you access a site that uses techniques to secure the information between the website and yourself, Action Learning can read the information and remove inappropriate content or prevent access to the material. Excluded from this inspection are sites that contain sensitive financial information, including banks and payment systems. Your activity on the internet is closely monitored by the school, logs are kept of activity, whether on a school device or using your own device through the school Wi-Fi. These logs include who is accessing what material for how long from which device. The school email system is provided for educational purposes. Acceptable Use Policy Agreement I understand that I must use Action Learning's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people. For my professional and personal safety: I understand that Action Learning will monitor my use of the ICT systems, email and other digital communications. I understand that the rules set out in this agreement also apply to Action Learning ICT systems (eg laptops, email, etc) out of school, and to the transfer of personal data (digital or paper based) out of school. I understand that Action Learning's ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person. I will be professional in my communications and actions when using Action Learning ICT systems: I will not access, copy, remove or otherwise alter any other user's files, without their express permission. I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the Action Learning website) it will not be possible to identify by name, or other personal information, those who are featured. I will

I will only use chat and social networking sites in school in accordance with the school's policies. I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner. I will not engage in any on-line activity that may compromise my professional responsibilities. Action Learning has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school: When I use my mobile devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. I will not use personal email addresses on the school ICT systems. I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes). I will ensure that my data is regularly backed up, in accordance with relevant school policies. I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials. I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work. I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. I will not disable or cause any damage to school equipment, or the equipment belonging to others. I will only transport, hold, disclose or share personal information about myself or others as outlined in the school E-Safety Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage. I understand that Data Protection Policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority. I will immediately report any damage or faults involving equipment or software, however this may have happened. I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school. I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name _____

Signed _____

Date _____

Acceptable User Agreement – Student



Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Action Learning will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

This policy applies to any device in school. It applies across the whole network and includes WiFi. Action Learning carries out secure content inspection (SSL inspection). This means that when you access a site that uses techniques to secure the information between the website and yourself, Action Learning can read the information and remove inappropriate content or prevent access to the material. Excluded from this inspection are sites that contain sensitive financial information, including banks and payment systems. Your activity on the internet is closely monitored by the school, logs are kept of activity, whether

on a school device or using your own device through the school Wi-Fi. These logs include who is accessing what material for how long from which device.

Acceptable Use Policy Agreement

I understand that I must use Action Learning ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that Action Learning will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand Action Learning systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

I will not use Action Learning systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so. I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission. I recognise that Action Learning has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of Action Learning:
- I will only use my own personal devices (mobile phones/USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed. When using the internet for research or recreation, I recognise that:
- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me. I understand that I am responsible for my actions, both in and out of school:
- I understand that Action Learning also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. Please complete the sections to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student Name _____

Signed _____

Date _____