E-Safety Policy

Policy created on 1/9/2016 by D Hales

Policy Amended 04/03/2020 by D Chell

Policy updated 6/10/2022 and 9/6/2024 and 20/05/2026

Reviewed By	Date	Signature
Danielle Chell	09/06/2024	D Chell
Danielle Chell	02/06/2025	D Chell
Danielle Chell	20/05/2026	D Chell

Contents:

Statement of intent

At Alpha Learning we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the School recognises the importance of promoting the use of computer technology throughout the curriculum, we also recognise the need for safe internet access and appropriate use.

Our School has created this policy with the aim of ensuring appropriate and safe use of the Internet and other digital technology devices by all pupils and staff.

The School is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

This policy will operate in conjunction with other important policies in our Provision, including our Anti-bullying Policy, Data Protection Policy, Child Protection and Safeguarding Policy, Allegations Against Staff Policy.

1. Legal framework

1.1. This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- The Data Protection Act 2018
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Keeping children safe in education 2024

2. Use of the internet

2.1. The School understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for academies to implement, which minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. These risks include:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to pupils or staff, due to inappropriate internet access or use both inside and outside of Alpha and to deal with incidents of such as a priority.

3.2. The e-safety officer, Danielle Chell, is responsible for ensuring the day-to-day e-safety in our Provision, and managing any issues.

3.3. The head of centre is responsible for ensuring that the e-safety officer and any other relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff.

3.4. The e-safety officer will provide all relevant training and advice for members of staff on e-safety.

3.5. The head of centre will ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in the school.

3.6. The e-safety officer will regularly monitor the school of e-safety in the school and return this to the head of centre.

3.7. The School will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

3.8. Cyber bullying incidents will be reported in accordance with the Provision's Anti-Bullying Policy.

3.9. The e-safety officer will ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.

3.10. The management team will hold regular meetings with the e-safety officer to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs.

3.11. The management team will evaluate and review this E-safety Policy on a annual basis or as required.

3.12. The head of centre will review and amend this policy with the e-safety officer, taking into account new legislation and government guidance, and previously reported incidents to improve procedures.

3.13. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.14. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.

3.15. All staff and pupils will ensure they understand and adhere to the Acceptable Use Policy, which they must sign and return to the head of centre.

3.16. Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.

3.17. The head of centre is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

4. E-safety control measures

4.1. Educating pupils:

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring pupils are aware of the safe use of new technology both inside and outside of the Provision.
- Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.

4.2. Educating staff:

- All staff will undergo e-safety training on an annual basis to ensure they are aware of current e-safety issues and any changes to the schoolof e-safety.
- All staff will undergo regular audits by the e-safety officer in order to identify areas of training need.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand the E-safety Policy.

4.3. Internet access:

- Internet access will be authorised once parents and pupils have returned the signed consent form as part of the Acceptable Use Policy.
- A record will be kept by the head of centre of all pupils who have been granted internet access.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity. We use SENSO a Uk Safer Internet recommended provider, this system allows staff to monitor a students computer in real time and to take control of the system.

- Effective filtering systems will be established to eradicate any potential risks to pupils through access to particular websites. SENSO has an established complete category of filtered words and phrases, however staff have the ability to add new words or phrases if they become aware of them almost instantly.

- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the head of centre, however staff can instantly block access using there SENSO management page while in a lesson.

    - SENSO records all student attempts to access blocked or filtered sites and produces a report for the Head Of Centre, creating a immediate warning to class teacher and Head of Centre if a Critical level. The Head of Centre is then able to link the alert to My Concern directly from the software. This is then processed correctly according to the E Safety/Behaviour/ Safeguarding Policy as Appropriate.

- All school systems will be protected by up-to-date virus software.

- An agreed procedure will be in place for the school of temporary users, e.g. volunteers.

- The master users' passwords will be available to the head of centre for regular monitoring of activity. We also use an outside IT specialist company ACC IT who are able to access all the computers as required, and enable to provide specialist knowledge if needed.

4.4. Email:

- Pupils and staff will be given approved email accounts and are only able to use these accounts.

- Use of personal email to send and receive personal data or information is prohibited.

- No sensitive personal data shall be sent to any other pupils, staff or third parties via email.

- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.

- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

4.5. Social networking:

- Access to social networking sites will be filtered as appropriate. SENSO currently blocks all social media sites on student computers.

- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the head of centre.

- Pupils are regularly educated on the implications of posting personal data online, outside of the Provision.

- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the School as a whole.

- Staff are not permitted to communicate with pupils over social networking sites.

4.6. Published content on the School website and images:

- The head of centre will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.

- All contact details on the School website will be the phone, email and address of the Provision. No personal details of staff or pupils will be published.

- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.

- Pupils are not permitted to take or publish photos of others without permission from the individual.

- Staff are able to take images, though they must do so in accordance with School policies in terms of the sharing and distribution of such.

Staff will not take images using their personal equipment.

4.7. Mobile devices:

- The head of centre may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.

- Mobile devices of students must be handed in at reception in the morning on entering the building, they will be returned to students at the end of the day.

- Staff mobiles will be kept out of sight as per the Mobile Phone Policy

- The sending of inappropriate messages or images from mobile devices is prohibited.

- Mobile devices must not be used to take images or recordings of pupils or staff.

- The School will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

5. Cyber bullying

5.1. For the purpose of this policy, “cyber bullying” is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.

5.2. The School recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

5.3. The School will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

5.4. The School will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

5.5. The School has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-bullying Policy.

5.6. The head of centre will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

6. Reporting misuse

6.1. Misuse by pupils:

- Teachers will manage behaviour in line with the behaviour policy for students who engage in misbehaviour with regards to internet use as per the behaviour policy.

- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the head of centre, using the appropriate method My Concern/Incident report/Conversation.

- Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents/carers explaining the reason for suspending their internet use.

- Complaints of a child protection nature shall be dealt with in accordance with our Safeguarding Policy.

6.2. Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the head of centre, using My Concern and/or discussion with the Head of Centre.

- The head of centre will deal with such incidents in accordance with the Allegations Against Staff Policy, and may decide to take disciplinary action against the member of staff.

- The head of centre will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

Appendix 1 **E-Safety Agreement**

Alpha Learning understands the importance of students being able to use the internet for education and personal development. This includes social media platforms, games and apps. We aim to support students and young people in making use of these in their work. However, we also recognise that safeguards need to be in place to ensure students are kept safe at all times.

This agreement is part of our Code of Conduct for students, and staff. It also fits with our overarching Online Safety Policy.

Student: please read the following agreement and discuss it with your parents/carers and Alpha staff if there is anything you do not understand.

Parents/Carers: please read and discuss this agreement with your child and then sign it, ask your child to sign it, and return it to the Alpha Learning.

If you have any questions or concerns, please speak to **Nadine Wedgwood** (Head of Centre).

Student Agreement

- I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access and the language I use.
- I will not use social media during school time and will never distribute images of school or other students on social media, without permission.
- I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to the staff member.
- I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- I will not give out any personal information online, such as my name, phone number or address.
- I will not reveal my passwords to anyone.
- I will not arrange a face-to-face meeting with someone I meet online, unless I have discussed this with my parents/carers and/or staff and am accompanied by a trusted adult.
- If I am concerned or upset about anything I see on the internet, or any messages that I receive, I know I can talk to any member of staff at Alpha.

I understand that my internet use at Alpha Learning will be monitored and logged and can be made available to staff. I understand that these rules are designed to keep me safe and that if I choose not to follow them, Alpha Learning may contact my parents/carers or other authorities such as the Police, depending on the severity of the breech.

We have discussed this E-Safety Agreement and …….(student name) agrees to follow the rules set out above.

Parent/Carer Signature…… **Date** ……

Student's Signature…… **Date** ……