ASHWOOD
SPENCER ACADEMY

Online Safety Policy

September 2020

Ashwood Spencer Academy online safety policy

This document should be read in conjunction with the: Why and how we teach online safety @ Ashwood Spencer Academy (appendix 1).

Online safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users, to enable them to control their online experience.

This policy should be read in conjunction with other policies including: the behaviour policy; the safeguarding policy, the computing (subject) policy and the document titled: Why and how we teach online safety @ Ashwood Spencer Academy (please see this in appendix 1).

Writing and reviewing the online safety policy

The Online Safety Policy is important to the School Development Plan and relates to other policies including those for Computing and for child protection.

- The school will appoint an online safety Coordinator. At the time of writing, this is the Computing Subject Leader.
- Our Online Safety Policy has been written by the school, building on local and national guidance including that from the Computing Subject Leaders group, the Spencer Academies Trust and government. It has been agreed by the senior leadership and approved by governors.
- The Online Safety Policy will be reviewed every 2 years.

Teaching and learning

Why internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. Ashwood Spencer Academy recognises that it has a duty to provide children and young people with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool in teaching and learning for staff and pupils.

Internet use will enhance learning

- The school's internet access is available to enhance the teaching and learning in school. It is designed explicitly for pupil use and includes excellent filtering, appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and will be given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in all online activities that will support the learning outcomes planned for the pupils' age and maturity. Staff will also educate them in the effective use of the internet for research, including the skills of knowledge location, retrieval and evaluation. **It is important that pupils learn not to copy information from the internet (plagiarise) but use it to inform their written work.**

Pupils will be taught how to evaluate internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to: AIT Services, and (where appropriate) the school's Online Safety Coordinator.
- The school will ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses BT Broadband provided by AIT services with its firewall and filters.

Use of Email (pupils)

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.
- Use of 'banned' words is detected and logged through the school's internet filtering system.
- Emails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The contact details on the school website or the learning portal will be the school address, email and telephone number. Staff or pupils' personal information should not be published in line with GDPR guidance.
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing staff and pupil's images and work

- Photographs that include pupils will be selected carefully and where individual pupils are identifiable, these children must have prior agreement from parents/carers.
- Pupils' full names must not be used anywhere on the website, particularly in association with photographs, initials of children should be used in all correspondence.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or published via social media (for e.g. on Twitter).
- Pupil's work can only be published with the permission of the pupil and their teacher.
- Images of staff will not be published without the individual's prior consent.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils will be taught never to give out personal details of any kind, which may identify them or their location, this is in line with the SMART internet safety objectives taught throughout school. Examples would include use of: real name; address; mobile or landline phone numbers; name of school; IM address; email address; names of friends; specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils. Parents will be informed by a relevant member of staff if the use of social networking is inappropriate and appropriate guidance can and will be given.

Managing filtering

- The school will work in partnership with the AIT Services to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to AIT Services and (where appropriate) the school Online Safety Coordinator.
- The Online Safety Coordinator, with support from senior staff, will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. (*Note: There is a danger in 'testing' the system to try to access inappropriate materials as when it is picked up by AIT it will be traced back and the perpetrator will then have to prove their innocence! It is advisable that AIT are notified of such tests* ***BEFORE*** *these checks are due to commence).*

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed where appropriate.
- Mobile phones will not be used during lessons or during 'official' school time. Staff are aware that personal mobile phones can be used in the staff room at break and lunch times but must not be used during lesson times and must not be used for the recording of pupils. The sending of abusive or inappropriate text messages is forbidden.
- School phones will be made available as and when staff are required to contact parents/carers. If staff choose to use their own personal devices (outside of teaching hours) they are advised to do so using the 'no- caller ID' option.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and in line with GDPR regulations.

Policy Decisions & Responsibilities

Authorising Internet access

- All internet use in school by pupils **MUST** be supervised.
- The school **WILL** maintain a current record of all staff and pupils who are granted internet access.
- All users **MUST** read and abide by the **age appropriate Acceptable Use Policy** on an annual basis.
- In EYFS and Key Stage 1, access to the internet **WILL** be by adult demonstration (where necessary) with directly supervised access to specific, approved online materials.
- In KS2 it is appropriate, at certain times, for pupils to access the internet with more freedom. Pupils **MUST** be made aware that failure to follow the expectations for correct internet usage **MAY** lead to internet restrictions in the future.

- Parents WILL be asked to sign and return a consent form to show they have read, discussed and ACCEPTED the Acceptable Use Policy on behalf of their child/ren.

Assessing risks

- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school WILL take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the Trust can accept liability for the material accessed, or any consequences of internet access.
- The Principal and Online Safety Coordinator WILL ensure that the Online Safety Policy is implemented and compliance with the policy monitored.

Handling online safety complaints

- Complaints of Internet misuse by pupils WILL be dealt with by a senior member of staff. In the first instance this may be the Computing Subject Leader, Year Group Director or a member of SLT. The Principal WILL be informed about all incidents. A log of such incidents WILL be maintained on CPOMs and parents MAY be made aware.
- Any complaint about staff misuse MUST be referred to the Principal who WILL use the agreed Trust procedures.
- Complaints of a child protection nature WILL be dealt with in accordance with agreed child protection and safe guarding procedures.
- Pupils and parents WILL be informed of the complaints procedure.
- Sanctions for internet misuse MAY include:
  - recording the incident on CPOMs
  - informing parents or carers;
  - removal of internet or computer access for a certain time period.

Community use of the Internet

- The school WILL liaise with local organisations to establish a common approach to online safety as and when the need arises.
- The school WILL work with Trust partners through the Computing Subject Leaders group to share best practice and stay up-to-date with new developments, programs and resources.
- The school WILL be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and WILL offer appropriate advice to pupils and parents.

Communications Policy

Introducing the online safety policy to pupils

- Agreed rules for Internet access will be made available to all teachers to share with their pupils. Teachers may decide to display these agreed rules in their classroom.
- Pupils will be informed that internet use will be monitored and appropriate filters are in place.
- **Online Safety will be taught by all teaching staff to support the understanding of online safety to all pupils.**
- An online safety training programme has been provided and delivered by the Online Safety Coordinator helping to raise the awareness and importance of safe and responsible internet use by all staff and pupils in school. (July 2020)

Staff and the Online Safety policy

- All staff will be asked to read and action the School's Online Safety Policy using CPOMs.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using the internet at school and when using school equipment to access the internet at home.

Enlisting parents' support

- Parents' attention will be drawn to the School's Online Safety Policy via the school's website and parents will be invited to attend Online Safety Training to support their understanding of Online Safety, the importance of it and how to support their children to become safe, responsible internet users.
- Resources offering further guidance, for parents and carers, to support them in providing safe internet use for their children will be shared at regular intervals throughout the school year and will be made available on class dojo, Twitter and the school's website.

Written by: Timothy Beer, Computing subject leader

July 2020 (Review date: August 2022)

Appendix 1: Why and How we teach Online Safety at Ashwood Spencer

1. What is online safety

Online safety, often referred to as 'internet safety', 'e-safety' or 'web safety', is usually defined as the safe and responsible use of computing technologies. This includes a range of different technologies and the use of the internet and encompasses the use of communication technologies using electronic media (e.g. text messages, gaming devices, email etc.).

In practice, online safety is as much about one's behaviour as it is about one's electronic security. Online safety in this context is categorised into three potential areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

2. Why we teach online safety at Ashwood Spencer Academy

As educators, we have an obligation to keeping our children and young people safe from harm online. But since 2012, OFSTED added online safety to their school inspection requirements and these requirements extended way beyond the classroom, encompassing the "whole school community" within the schools expected scope of delivery. Therefore, our obligation is not only to children and young people, but to parents, carers, governors and indeed all school staff, not just those involved in the direct education of pupils.

Our online safety aims:

- To enable children and young people to be responsible for their use of the Internet.
- To help children and young people develop internet skills and use information they find online wisely and sensibly.
- To ensure we develop respectful and considerate internet users.
- To help children and young people avoid embarrassment or humiliation when online.
- To keep children and young people safe from predatory adults.
- To help children and young people avoid physical danger.
- To educate children and young people about the dangers of becoming victims of crimes such as identity theft and fraud.
- To stop children and young people developing 'unhealthy' behaviours such as obsessive use of the internet or digital games.

Children and young people are often capable of using safe strategies, but as teachers, we need to be sure that children know what to do to STAY SAFE ONLINE.

Many young people have the technical skills to deal with online safety but they sometimes lack the wisdom to know when there is danger or how to deal with difficult situations if/when they arise.

Adults: teachers, parents and carers, are sometimes over-cautious or over-protective in their responses to these dangers. The Byron review – *Safer Children in a Digital World* (2007) highlights the need to help children and

young people tackle these issues rather than keep them protected from them and therefore prevent them learning how to deal with issues that arise.

In teaching online safety, we will endeavor to strike a balance between encouraging the safe use of computing technologies and making children fearful of potential consequences. The aim is not to discourage use of these technologies *BUT* to give children the experience, skills and knowledge to use it sensibly and safely. The Internet is a powerful and exciting tool and, when used with safety guidelines in place, provides many benefits to children and young people.

We also have an obligation to supporting children, young people, parents and carers so that they know **where** to turn to get support and **who** to report damaging behaviours to, when they have been experienced online.

3. What should be taught and how?

The teaching of online safety should focus on the following 3 areas:

- **Content:** educating our children and young people about how to deal with illegal, inappropriate or harmful materials, if they come face-to-face with these online.
- **Contact:** enabling our learners to know how to avoid the dangers of harmful online interaction with other users and the potential harms this may cause.
- **Conduct:** ensuring our children and young people are aware of their personal online behaviour and the consequences of not being a respectful internet user.

Online Safety covers a broad range of aspects including: **physical safety**, legal aspects such as **copyright** and **technical issues such as filtering.** Some aspects of Online Safety are built into our current teaching practice with all teachers responsible for covering the subjects on a regular basis (at least annually as highlighted in the school's Computing Long Term Plan). Most of this teaching will probably be during computing teaching time but can be done as part of other subjects for e.g. PSHE.

Staff are encouraged to look for cross-curricular links when covering Online Safety to strengthen children and young people's understanding of the subject through PSHE, citizenship, literacy and other subjects.

At Ashwood Spencer Academy our teaching of Online Safety follows SMART objectives (see appendix 2) and has always been progressive. Young children receive much more supervision and guidance and more protection than older children when using the internet. However, as children become more independent learners, teachers are encouraged to trust children with using the internet in a more independent nature and with increasing regularity. CHILDREN IN KS2 MUST BE TAUGHT ABOUT THEIR RESPONSIBILITY - and with it the freedom to explore, improving knowledge and skills as children progress up through the school.

At the heart of our Internet Safety teaching is the **Acceptable Use Policy** for the Internet. We have 3 such policies which reflect our progressive teaching of online safety. The Acceptable Use Policy for EYFS, KS1 and KS2 are shared with parents/carers annually and parents are encouraged to return signed slips to show that this has been read, understood and discussed with their child/ren.

Rules for using the internet safely are shared with pupils by teacher and teachers may wish to display these rules in their classrooms. These rules are also published on iPad and laptop trolleys and in the Computing Cupboard, where equipment is centrally stored. The rules outline safe and responsible behaviour online and should be reinforced through many subjects and on a frequent basis, particularly on occasions when pupils use the internet.

Many safety issues in schools rely on a partnership between parents/carers and teachers. As a school, we want to work with parents and carers to help them to help their children to stay safe at home as well as at school. Links to additional information are shared by teachers on class dojo and may be published on the school's website too. Links for children are provided via the learning platform.

4. How are we doing at Ashwood Spencer Academy?

A good way to see how our school fairs against the OFSTED requirements is to ask ourselves these 5 questions:

1. How do you ensure that all staff receive appropriate online safety training that is relevant and regularly up to date?
2. What mechanisms does the school have in place to support pupils and staff facing online safety issues?
3. How does the school educate and support parents and whole school community with online safety?
4. Does the school have e-safety policies and acceptable use policies in place? How does the school know that they are clear and understood and respected by all?
5. Describe how your school educates children and young people to build knowledge, skills and capability when it comes to online safety? How do you assess its effectiveness?

We are currently in the process of reviewing some of the 5 above measures for assessing our school's Online Safety practice. This will help us to ensure that it meets the needs of our learners.

Appendix 2: SMART Online Safety Objectives


Stay Safe Online
Remember the 5 SMART rules when using the internet and mobile phones.
S
SAFE: Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.
m
MEET: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
a
ACCEPTING: Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
r
RELIABLE: Information you find on the internet may not be true, or someone online may be lying about who they are. Make sure you check information before you believe it.
t
TELL: Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
Find out more at Childnet's website …
www.kidsmart.org.uk
Childnet International © 2002-2007 Registered Charity no. 1080173 www.childnet.com
Childnet International
Kid Smart

- Kidsmart http://www.kidsmart.org.uk/

Kidsmart is an award-winning practical internet safety programme website for schools, young people, parents, and agencies, produced by the children's internet charity Childnet International.

- Hector's World http://www.thinkuknow.co.uk/5_7/hectorsworld/

An excellent website that outlines all the dangers to children online and how to tackle each one in turn. Aimed at parents but equally relevant for teachers.

- Child Exploitation and Online Protection Centre http://www.ceop.police.uk/

The Child Exploitation and Online Protection (CEOP) Centre works across the UK and maximises international links to deliver a holistic approach that combines police powers with the dedicated expertise of business sectors, government, specialist charities.

- Get Safe Online https://www.getsafeonline.org/

Get Safe Online will help you protect yourself against internet threats. The site is sponsored by government and leading businesses working together to provide a free, public service.

- Grid Club – Cyber Cafe http://www.gridclub.com/v3/#/teacher

Pupils can visit different areas within the cyber café to find out top tips about how to stay safe when sending emails, text messages, instant messages and contributing to online forums.

- Netsmartzkids http://www.netsmartzkids.org/LearnWithClicky

Pupils can watch animated videos in which Clicky the robot teaches them how to stay safe online.

- Disney Safesurfing http://www.disney.co.uk/DisneyOnline/Safesurfing/child-home.html

Disney Online's Safe Surfing with Doug, featuring an animated Disney character, uses a variety of fun, interactive tools to help children and young people learn e-safety messages.

- Think U Know https://www.thinkuknow.co.uk/

This website is created by the Child Exploitation and Online Protection (CEOP) Centre and contains loads of information on how to stay safe online. Many topics are covered – including mobiles, blogging and gaming sites.

- Digizen http://www.digizen.org/

An excellent website that promotes digital citizenship and has useful resources for teachers. Signposts to safety: Teaching e-safety at Key Stages 1 and 2? This is an excellent document produced by BECTA that outlines all the dangers to children online and how to tackle each one in turn.

*Please note: There are separate Acceptable Use Policies for EYFS, KS1 and KS2.

Ashwood Spencer Academy Acceptable Use Policy for Children in KS2

We want all children to feel safe online, always. One of the ways we can achieve this is through our Acceptable Use Policy, which sets out key rules for our internet use in school.

I agree that I will:

- ✓ Always keep my passwords secret.
- ✓ Only move and share personal data securely.
- ✓ Only visit sites, which are appropriate.
- ✓ Work in collaboration only with people my school has approved and I will deny access to others.
- ✓ Respect the school network security.
- ✓ Make sure all messages I send are respectful, considerate and non-offensive.
- ✓ Show a responsible adult any content that makes me feel uncomfortable.
- ✓ Not reply to any nasty message or anything that makes me feel uncomfortable.
- ✓ Not use my own mobile device in school unless I am given permission.
- ✓ Only give my mobile phone number to friends I know in real life and trust.
- ✓ Only e-mail people I know or who are approved by my school.
- ✓ Only use e-mail which has been provided by school.
- ✓ Always follow the terms and conditions when using a website.
- ✓ Always keep my personal details private (my name, family information, journey to school, sports clubs I belong to …. are all examples of personal information).
- ✓ Always check with a responsible adult before I share images of myself or others.
- ✓ Only create and share content that is legal.
- ✓ Never meet an online friend without taking a responsible adult that I know with me.

I understand that everything I do on the computer can be seen by others.

- *I am aware of what the CEOP report button is and I know when to use it.*
- *I know that anything I share may be monitored.*
- *I know that once I share anything online it is completely of my control and may be used by others in a way that I did not intend.*
- *I am aware that my actions online, in school and out of school, are monitored and incorrect use of computers in school could lead to: incidents being logged on CPOMs; pupil and parent meetings and/or internet restrictions being imposed during school time.*

Ashwood Spencer Academy Acceptable Use Policy for learners in KS2 (reviewed 2020)

PARENTS, PLEASE DISCUSS THE ABOVE RULES WITH YOUR CHILD TO ENSURE HE OR SHE UNDERSTANDS THEM. PLEASE CONTACT SCHOOL IF YOU REQUIRE FURTHER GUIDANCE OR SUPPORT WITH THIS.

I have read this document and I understand what I should do to keep myself safe. I also

I acknowledge that I have received a copy of the Ashwood Spencer Academy Acceptable Use Policy for learners in KS2 and have discussed it with my child. I understand that my child will engage in activities in school to help them to understand these rules and to develop safe behaviours when working online. I also **understand that my child must ask a responsible adult if they are not sure about something when using the internet.**

Signed (parent): .....

Signed (pupil): .....

Parent / carer of: .....

Date: .....