Digital Safety Policy

E Safety Policy (Including EYFS)

Policy Review Date: Sept 2022
Reviewed By: M Ashron & SLT
Next Review: Sept 2023 (or following incident, legislation or interim guidance)

Distribution

Please note that 2 copies of this policy are printed as standard and distributed to the following areas:

1) Staff Room
2) School Office

This policy is also made available on the school website.

Updates and Amendments to Policy

Date	Section Heading	Update Details	Page N°
28/01/2019	4) Pupils Evaluation of Internet content	If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Computing Coordinator. i. The Computer Coordinator must then complete an incident section in the 'Online Safety Log'. ii. The Computer Coordinator will review the incident and take appropriate course of action. This may include adjusting filtering, reviewing policies, asking for assistance from Pro- Networks, sharing experience with staff and/or parents/carers and applying sanctions. iii. The incident will be reported to the SLT. If staff or pupils discover Illegal material the Computing Coordinator and Designated Safety Lead must be informed immediately. i. Procedures will be followed as above when discovering unsuitable sites. ii. If a child is at risk procedures will be followed according to the 'Safeguarding Children and Chid Protection Policy' and 'Keeping Children Safe in Education Part 1' iii. The incident will also be reported to CEOPs.	6
28/01/2019	5) Management of e-mail	pupils must immediately tell a teacher if they receive offensive e-mail. The teacher must then report it to the Computing Coordinator who must complete an incident section in the 'Online Safety Log' and review the incident as stated in section 4);	6
28/01/2019	Appendix 2	Incident sheet from Online Safety Log	11
11/3/2020	2.2 How the Internet benefits education.	Access to educational online programs.	5
15/9/2022	Significant review	Updating of all areas	

CONTENTS

This policy applies all staff, volunteers and pupils in the School, including in the EYFS & Wraparound.

Computing Coordinator: Miss L McFerran
Designated Safeguarding Lead: Mrs Joanna Callaway (Headteacher)

RATIONALE

i) Internet Policy

Avalon School believes in the educational benefits of curriculum Internet use. Good planning and management that recognises the risks will help to ensure appropriate, effective and safe pupil use. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail in order to enable pupils to learn how to locate, retrieve and exchange information using ICT. Computer skills are vital to access life-long learning and for future employment.
Most technologies present risks as well as benefits. Internet use for home, social and leisure activities is expanding and being used by all sectors of society. This brings young people into contact with a wide variety of influences, some of which could be unsuitable. It is important that Schools, as well as parents, adopt strategies for the responsible and safe use of the Internet.

ii) Core Principles of Internet Safety

The Internet has become as commonplace as the mobile phone or TV and its effective use is an essential life-skill. Unmediated Internet access brings with it the possibility placing of pupils in embarrassing, inappropriate and even dangerous situations. This policy aims to help to ensure responsible use and the safety of pupils. It is built on the following five core principles:

iii) Guided Educational Use

Significant educational benefits should result from curriculum Internet use including access to information from around the world and the ability to communicate widely and to publish easily. Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

iv) Risk Assessment

21st Century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they need to learn to recognise and avoid these risks - to become “Internet Wise”. Pupils need to know how to cope if they come across inappropriate material.

v) Responsibility

Internet safety depends on staff, Schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and associated communication technologies. The balance between education for responsible use, regulation and technical solutions must be judged carefully.

vi) Regulation

The use of a limited and expensive resource, which brings with it the possibility of misuse, must be regulated. In some cases access within School is denied, for instance unmoderated chat rooms present immediate dangers and are banned. Fair rules, clarified by discussion and prominently displayed help pupils make responsible decisions for both School and home access.

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL/ DDSL) are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the staff in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Computing lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT management system

In conjunction with Obsidian Networks, the school is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher (DSL)

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their classes

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or

- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the headteacher is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the headteacher should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to Headteacher (DSL) to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

Appendix 1 – Acceptable Computer Use Policy, included in the Safeguarding booklet, sent out to Parent/Carers each academic year.

As part of your child's curriculum and the development of Computing skills, Avalon School provides supervised access to the Internet. We believe that the use of the World Wide Web and Email is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Acceptable Computer Use Policy and talk about them with your child as appropriate to their age. Then sign consent form so that your child may use the Internet at School.

We take positive steps to deal with this any risk of the children in our School having access to undesirable materials, including our Internet provider operating a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Our rules also concern the types of communications that children make using computers and other technology. We would like your support in helping to ensure that the children at the School are using technology in a responsible and polite manner and never in a way that could upset another person or spoil their work.

A full copy of our E-safety policy is on the School website or available in School should you require a copy.

Should you wish to discuss any aspect of Internet use please contact Mrs Ellsmoor, our Computing Coordinator, or you child's class teacher in the first instance.

Please read and discuss with your child then sign and return to the School.

- Children must ask permission before accessing the Internet.
- We expect all children to be responsible for their own behaviour on the Internet, just as they are anywhere else in School. This includes materials they choose to access, and language they use.
- Children must only use websites and search engines as directed by staff.
- Children are expected not to use any rude language in their email communications and contact only people the staff have approved.
- Children should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet.
- No programs on disc, memory drives etc. may be brought in to School and used without approval from staff first.
- Children not complying with these expectations will be warned, and subsequently, may be denied access to Internet resources.

E-Safety and the Internet

Nursery, Pre-School & Infant Children			
I have read through the agreement and gone through it as appropriate with my child and agree to adhere to it. Please sign below on behalf of your child:			
Signed by Parent/Carer:		Date:	

Junior Children			
I have read and understand the School Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.			
Signed by Child:		Date:	

Parent's Consent for Internet Access			
I have read and understood the School rules for responsible Internet use and give permission for my child to access the Internet. I understand that the School will take all reasonable precautions to ensure children cannot access inappropriate materials. I understand that the School cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the School is not liable for any damages arising from use of the Internet facilities.			
Signed by Parent/Carer:		Date:	

Appendix 2 – Incident sheet from Online Safety Reporting Log.

Online Safety Reporting Log.

Read notes 'Responding to incident of misuse'.

Incident				Action taken		
Date	Time	Incident	Incident reported by:	By who?	What action was taken?	Signature