
Ainslie Wood Primary School

Online Safety Policy

Contents

1. Introduction.....	1
2. Aims	2
3. Legislation and guidance	2
4. Roles and Responsibilities.....	2
5. Educating pupils about online safety	4
6. Parents and Online Safety.....	5
7. Cyber-bullying.....	5
8. Acceptable use of the internet in school	6
9. Social Media	7
10. Pupils using mobile devices in school	7
11. Staff using work devices outside school	8
12. How the school will respond to issues of misuse.....	8
13. Training	8
14. Monitoring arrangements	9
15. Links with other policies	9

1. Introduction

Technology skills are vital to access life-long learning and employment; indeed ‘computer literacy’ is now seen as an essential life-skill. The Internet and IT are essential resources to support teaching and learning at Ainslie Wood Primary. The curriculum requires pupils to learn how to locate, retrieve and exchange information safely. In delivering the curriculum, teachers integrate the use of technology such as web- based resources and devices including tablets and laptops.

Young people have access to the Internet from many places including home, school, friends’ homes, libraries and, in many cases, personal, portable equipment such as mobile phones and tablets. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to access the internet safely. This policy is designed to ensure safe internet use by pupils in school, but also while on-line at other times.

Internet safety depends on governors, staff, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies such as mobile phones. There are no straightforward or totally effective

solutions and staff, parents and the pupils themselves must remain vigilant.

2. 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

3. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the Department'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](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

4. Roles and Responsibilities

4.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation including monitoring online safety incidents 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 IT systems and the internet

4.2 The designated safeguarding lead

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the School Business Manager, IT support technician and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMs and are dealt with appropriately in line with the school relationship policy and safeguarding policy
- Ensuring up-to-date staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing reports on online safety in school to the governing board

4.3 The School Business Manager/IT support technician

The School Business Manager/IT support technician are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT 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 IT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

4.4 All staff and volunteers

All staff, including 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 IT 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 on CPOMs 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

4.6 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 IT systems and internet

Parents can seek further guidance on keeping children safe online. For up-to-date advice please seek the advice of the designated safeguarding lead (DSL) or visit:

www.nspcc.org.uk

www.gov.uk

www.bbc.com

www.internetmatters.org

4.7 Visitors and members of the community

Visitors and members of the community who use the school's IT 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.

5. Educating pupils about online safety

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

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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

6. Parents and Online Safety

- This Online Safety Policy will be shared with parents via the school website.
- A partnership approach with parents will be encouraged through sharing of information for safe Internet use at home, including updated information when it is published. Internet issues will be handled sensitively to inform parents without undue alarm.
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Designated Safeguarding Lead, Philippa Ioannou.
- Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

7. Cyber-bullying

7.1 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

7.2 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 in class and in assemblies, explaining the reasons why it occurs, the forms it may take and what the consequences can be in.

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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services where it is deemed necessary to do so.

7.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete

inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

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

8. 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 IT systems and the internet. 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.

9. Social Media

Staff, Parents

To help ensure effective communication both within the school and outside of school, we expect everybody to engage respectfully on social media. This includes (but is not limited to) not making any posts which are or could be construed as bullying, use of aggressive or insulting language, any illegal or otherwise inappropriate behaviour, including the sharing of material which is harmful or in breach of confidentiality and/or GDPR rules.

Comments and posts on social media, including public and private forums, community, pupils' and parents' chats, pages or groups, which might cause distress or bring the school into disrepute should be avoided. If an individual has any concern regarding the school, it is urged that they contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed.

Pupils

Many social media platforms have a minimum age restriction of 13. Parents are asked to respect the age ratings on social media platforms and not encourage underage use. School must strike the difficult balance of not encouraging the underage use of social media or seeking to manage external incidents and parenting decisions, whilst acknowledging the reality in order to best support our pupils and families.

In the event that a member of staff becomes aware of a pupil having an inappropriate social media account, contact will be made with parents/carers informing them of the legal age requirement. Where we become concerned that a pupil is at risk of harm because of social media, we will follow Child Protection and Safeguarding Policy. We will seek intervention from the appropriate external agencies, which where appropriate, will include contacting the police. Harmful risk could include the following:

- Spam and other inappropriate e-mail
- Online Grooming
- Illegal activities of downloading or copying copyright materials
- Viruses
- Cyberbullying
- Sexting – the sending of indecent personal images, videos or text
- Abusive or pornographic online content
- Radicalisation and other movements
- Social, Emotional and Mental Health (SEMH) effects of an increased use of technology
- Groups that promote self-harm and/or eating disorders

10. Pupils using mobile devices in school

Pupils in Year 6 may bring mobile phones into school which are handed in for safe keeping during the entirety of the school day and they are not permitted to use them during:

- The school day
- Clubs before or after school, or any other activities organised by the school

Any use of other mobile devices in school by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger sanctions in line with the school relationship policy.

11. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

If staff have any concerns over the security of their device, they must seek advice from the School Business Manager.

Work devices must be used solely for work activities.

12. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding policy.

14. Monitoring arrangements

The DSL monitors behaviour and safeguarding issues related to online safety via CPOMs including analysing these against pupil cohorts including gender and ethnicity.

This policy will be reviewed every 2 years by the designated safeguarding lead (DSL). At every review, the policy will be shared with the governing board.

15. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Relationship policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use policy