Online safety policy

Arunside School

Approved by:	FGB (with P&R Focus)	**Date:** November 2023
Last reviewed on:	March 2022	
Next review due by:	November 2026	

Date	Section	Policy review updates:
21/03/22	Section 3.1	Replaced Bruce Glocking's name with Victoria Coward
21/03/22	Section 3.5	Replace: 'Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy' With 'Reporting incidents of cyber-bullying to the DSL, so that they can be dealt with appropriately in line with the school behaviour policy'
21/03/2022	Section 5	As the subscription is has not been renewed, (insufficient parents took up the offer) the following wording has been removed: 'The school has signed up with The Child Protection Company so that parents can access a free online Parent e-Safety course, to enable them to work with their child to keep them safe on the internet and learn more

		about e-Safety responsibilities as a parent. The link for this course is available through the school office.’
21/03/22	Section 6.1	Replace ‘(See also the school behaviour policy.)’ With (See the school behaviour policy for more details on sanctions and processes for dealing with bullying.)
21/03/22	Section 10	Incorporating the school’s policy on Social media into the Online Safety Policy. The sections on bullying and mobile phones and digital photography in the previous stand-alone social media policy has been removed as Section 6 of the Online Safety Policy deals with it adequately.
24/11/23	Section 3.1	Replaced Victoria Coward’s name with Luke Walters
24/11/23	Section 3.6	Remove due to broken link: Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
24/11/23	Throughout	Amend to reflect new title of Relationship and Behaviour policy
27/11/23	Section 5	Insert: The school has signed up to West Sussex Digital Safety Package and the National College’s ‘National Online Safety Training’.
24/11/23	Section 8	To reflect operational processes, remove: will be securely stored in the school office

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

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

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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.

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).

The governor who oversees online safety is Luke Walters

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 (appendix 2)

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) and deputies are set out in our child protection and safeguarding policy.

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

In ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Working with the ICT lead and other staff, as necessary, to address any online safety issues or incidents

Ensuring that any online safety incidents are logged (see appendix 4) 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 Relationship and Behaviour Policy

Updating and delivering staff training on online safety (appendix 3 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 lead

The ICT lead is responsible for:

Ensuring appropriate filtering and monitoring systems are in place, 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 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 monthly 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 (see appendix 4) 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's Relationship and Behaviour Policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

Maintaining an understanding of this policy

Implementing this policy consistently for learning both in-school and online teaching

Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)

Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

Reporting incidents of cyber-bullying to the DSL, so that they can be dealt with appropriately in line with the school's Relationship and Behaviour policy

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 (appendix 1)

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

- What are the issues? UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

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 (appendix 2).

4. 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

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school has signed up to West Sussex Digital Safety Package and the National College's 'National Online Safety Training'.

The School will raise parents' awareness of internet safety in letters or other communications sent home; through information on our website and through the virtual learning environment (VLE).

Online safety will also be covered during dedicated parents' briefings.

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

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

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See the school's Relationship and Behaviour policy for more details on sanctions and processes for dealing with bullying.)

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 when 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. Class teachers will discuss cyber-bullying with their class, and the issue will be addressed in assemblies.

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 their 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's Relationship and Behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure that 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 if it is deemed necessary to do so.

6.3 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.

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 and 2). 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 and 2.

8. Pupils using mobile devices in school

Year 6 Pupils may bring mobile devices into school, but are not permitted to use them during the school day. All mobile devices must be handed in at the start of the school day where they will be securely stored before being returned to the pupils at the end of the school day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school's Relationship and Behaviour policy, which may result in the confiscation of their device.

9. 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, as set out in appendix 2.

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. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT lead.

Work devices must be used solely for work activities.

10. Social media and social networking sites

Social media and social networking sites play an important role in the lives of many people and whilst it is recognised that the use of social networking websites bring risks, it is also acknowledged that there are many benefits to be reaped. The way in which social networking websites should be used by school staff, governors, visitors, parent helpers and pupils at Arunside Primary School falls under the three key areas of:

- **The use of social networking sites by pupils within school**
- **Use of social networking by staff and volunteers in a personal capacity**
- **Comments posted by parents/carers**

The use of social networking sites by pupils within school
In terms of private use - Children under the age of 13 are not permitted to be registered on social networking websites. This includes Facebook, Instagram and apps.

Social networking websites should not be used / accessed in school unless under the direction of a teacher, and for a purpose clearly linked to a relevant learning objective. If social media websites are being used by a class to aid learning, then staff should carry out a risk assessment to determine which tools are appropriate, and how they should be used.

Use of social networking by staff and volunteers in a personal capacity
It is possible that a high proportion of staff, governors and adult volunteers will have their own social networking site accounts. It is important to protect both the professional reputation of staff, and the reputation of the school by ensuring that personal accounts are used in an appropriate manner and do not conflict with responsibilities to Arunside School.

Staff, governors and volunteers must **never** add pupils as 'friends' into their personal accounts (including past pupils under the age of 16). Staff are **strongly advised** not to add parents as 'friends' into their personal accounts. Teaching Staff must not use social networking sites within lesson times (for personal use) and should only use social networking in a way that does not conflict with the current National Teacher's Standards.

It is not appropriate for staff, governors or volunteers to make comments about the school, pupils, parents or colleagues including members of the Governing Body. Neither should they post sensitive information, opinions about Arunside Primary School or pictures of school events. Privacy settings on all social media should be regularly reviewed to give an appropriate level of privacy and confidentiality, and ensure that it is maintained. Where staff or governors are directly asked for an opinion about the school on social media, a polite referral to the school's website for information, or the school office/Headteacher for comment, is appropriate. **Inappropriate use of social media should be referred to the Headteacher in the first instance and may lead to disciplinary action**.

Comments posted by parents/carers
Parents and carers will be made aware of their responsibilities regarding their use of social media. Methods of school communication include the prospectus, the website, newsletters, letters and verbal discussion.

School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

- Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.
- Parents should make complaints through official school channels rather than posting them on social networking sites.
- Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.
- We understand that parents use social media to network with each other and share information such as dates for events, topic or activity information, for example. We ask that this is done privately and with sensitivity, to ensure the privacy of pupils is always maintained.

11. Digital Photography

Children have their photographs taken to provide evidence of their achievements for their development records (The Early Years Foundation Stage, EYFS 2007). **Staff, visitors, volunteers and pupils are not permitted to use their own mobile phones to take or record any images of school children for their own records during the school day.**

Procedures

- Under the General Data Protection Regulations (GDPR), the school will notify parents that pupils may be photographed or filmed at school or on events/trips and the images/recordings may be used for educational purposes. The school will always seek parental consent to utilise images for other purposes, e.g. for the use of building passes or media promotions.
- Photographs and recordings stored on the school network, which is password protected, may be retained until the school ceases to operate, should this occur then all photographs will be shredded or deleted from the school network.
- The school's digital cameras and iPads must not leave the school setting (unless on an educational visit).
- Photographs are printed in the setting by staff and images are then removed from the camera memory.
- Many mobile phones have inbuilt cameras so staff mobile phones must not be used to take pictures of children in our school.
- **Visitors may only use their phones in the foyer or outside the building and should be challenged if seen using a camera inappropriately or photographing children.**
- The use of cameras and mobile phones are prohibited in toilets.
- Staff are asked not to make personal calls during their working hours when working directly with children. However, in urgent cases a call may be made or accepted if deemed necessary and by arrangement with the Head Teacher.
- All school cameras, iPads and videos should be kept securely at all times and used with appropriate authority.

12. How the school will respond to misuse of the School's ICT Systems or Internet

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the School's Relationship and Behaviour policy. 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 ICT 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, where applicable.

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

14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed every three years by the headteacher. 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:

Child protection and safeguarding policy (including the Addendum to this policy dated March 2020)

Relationship and Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school’s ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school’s ICT systems and accessing the internet in school, I will not:

Use them for a non-educational purpose

Use them without a teacher being present, or without a teacher’s permission

Access any inappropriate websites

Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)

Use chat rooms

Open any attachments in emails, or follow any links in emails, without first checking with a teacher

Use any inappropriate language when communicating online, including in emails

Share my password with others or log in to the school’s network using someone else’s details

Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer

Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher’s permission

I will ensure that it is handed into the school office at the start of the school day for secure storage until the end of the school day

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school’s ICT systems and internet responsibly.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school’s ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school’s ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school’s ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school’s ICT systems and accessing the internet in school, or outside school on a work device, I will not:

Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature

Use them in any way which could harm the school’s reputation

Access social networking sites or chat rooms

Use any improper language when communicating online, including in emails or other messaging services

Install any unauthorised software

Share my password with others or log in to the school’s network using someone else’s details

I will only use the school’s ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school’s data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school’s ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**