West Sussex Education Authority

Nyewood CE Infant School

"SMILING, CARING AND LEARNING TOGETHER ON A JOURNEY WITH GOD"

Online Safety Policy

Date: July 2022

Review: July 2024

Contents

---

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 (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;
- Harmful online challenges and online hoaxes.

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. 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 Body

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

The governing body 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 the safeguarding governor.

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 DSL and deputies 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 headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the headteacher, SLT and other staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safety incidents are logged on the school safeguarding recording system 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;
- Ensures the updating and delivering of 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 body.

This list is not intended to be exhaustive.

3.4 The IT Technician

The IT technician is 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;
- Ensuring that any online safety incidents are logged on the school safeguarding reporting system and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are reported so that they can be 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 IT 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 on the school safeguarding reporting system 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;
- Ensure they have an understanding of the remote learning policy;
- Ensure all staff are aware of the appendices and relevant policies (see section 15).

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 understood and agreed to the terms on acceptable use of the school's IT systems and internet (appendix 1);
- Ensure they follow the guidelines and rules during remote learning supporting their child where necessary;

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 factsheet - Childnet International;

- Healthy relationships – Disrespect Nobody.

3.7 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 (appendix 2).

3.8 Children

Children will ensure they follow the acceptable user policy they have understood with their parents and will apply their understanding of online safety that has been developed through online safety lessons.

Pupils will report to school staff anything they find uncomfortable or do not understand.

4. Educating Children About Online Safety

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

The introduction of E4S and the new Relationships and Sex Education (RSE) curriculum was compulsory from September 2020.

Under the new requirement, **all** schools have to teach:

- Relationships education and health education in primary schools.

This new requirement includes aspects about online safety. The expectations are listed below:

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.

The National Curriculum also states:

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.

The use of social media and the internet will also be taught in an appropriate way.

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 on the school website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher and, if necessary, the headteacher and/or the DSL.

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

6. Cyber-Bullying

This section should be read in conjunction with the Anti-Bullying and Cyber-Bullying Policy.

Anti-Bullying and Cyber Bullying Policy April 2022

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.

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. Class 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 relationship, sex, health 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 (see section 9 for more detail).

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 if it is deemed necessary to do so.

7. Authorising Internet Access

- All staff must read and sign the 'Acceptable Use Agreement' before using any of school ICT resources.
- All parents will be required to sign the home-school agreement prior to their children being granted internet access within school.
- All visitors and students will be asked to read and sign the Acceptable User Agreement prior to being given internet access within the school.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.

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 ICT systems and the internet (appendices 1& 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.

9. Training

All new staff members will receive training and copies of relevant policies, 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, 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 Child Protection and Safeguarding Policy.

10. Monitoring Arrangements

An important element of online-safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff, volunteers and pupils have a responsibility to report online-safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school has incident reporting procedures in place and record incidents of an e-Safety nature on the school safeguarding reporting system.

The DSL logs behaviour and safeguarding issues related to online safety on the school safeguarding reporting system.

This policy will be reviewed annually. At every review, the policy will be shared with the governing body.

11. Device and Mobile Use

The use of mobile technologies brings both real benefits and challenges for the whole school community. The school Acceptable Use Agreements for staff, pupils and parents/carers and visitors will consider the use of mobile technologies.

The school allows:

	School Devices			**Personal Devices**		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device[1]	Pupil/Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*Some*	*No*
Internet only				*No*	*Yes*	*Yes*
No network access				*No*	*Yes*	*No*

Users of personal devices are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements. In addition, when <u>personal devices</u> are permitted:

- *Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user as does the liability for any loss or damage resulting from the use of the device in school.*
- *The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).*
- *The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues.*
- *The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security.*
- *The school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.*
- *Devices may not be used during lesson time or in front of the pupils, unless in exceptional circumstances and allowed by SLT.*
- *Devices must be in silent mode on the school site unless permitted by SLT.*
- *Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements.*
- *Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.*

- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity and only using school devices. Users must be aware of photographic restrictions. All unnecessary images or videos will be deleted immediately.
- Printing from personal devices will usually not be possible.
- Staff are not permitted to use their own mobile phones or devices for contacting pupils or their families within or outside of the setting in a professional capacity.
- In the case of school productions, parents/carers are permitted to take pictures of their child in accordance with school protocols, which strongly advise against the publication of such photographs on social networking sites.

Pupils' Use of Personal Devices

- Pupils are not permitted to bring a mobile device of any kind into school.

Users of school devices are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements. All staff members will take appropriate steps to ensure school devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date – always install the latest updates.
- Keeping the software / apps originally installed by the school on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson.
- Being mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Reporting any pop-ups or unusual action on any school device to the SBM or IT technician.
- Keeping the devices safe and locked away when not in use, particularly overnight.
- Teaching pupils how to use the devices safely before using them.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT technician/SBM.

12. Social Media

The school respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

- SLT are responsible for approving social media account creation in relation to the school;
- The social media account administrator/moderator is responsible for storing the account details securely and monitoring and contributing to the account;
- SLT are responsible for making an initial assessment when an incident is reported;
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school;
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate;
- The school will take appropriate action in the event of breaches of the Online Safety policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy;
- School blogs or social media sites should be password protected and approved by a member of the Senior Leadership Team or a member of staff that has been granted permissions.

Use of Images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected;
- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts following permissions given;
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published;

- *If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.*

Personal Use

Staff

- *Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer.*
- *Personal communications, which do not refer to or impact upon the school are outside the scope of this policy.*
- *The school permits reasonable and appropriate access to private social media sites away from the children and not during lesson time.*
- *The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.*
- *Staff will not post content or participate in any conversations, which will be detrimental to the image of the school. Staff who hold an account should not have parents or pupils as their 'friends'.*

Pupils

- *Staff are not permitted to follow or engage with current pupils of the school on any personal social media network account.*
- *The school's internet safety planning and teaching should enable the pupils/students to be safe and responsible users of social media.*

Parents/Carers

- *If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.*
- *Parents/carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parent/carers to the school's complaints procedures.*

13. *E-Mail*

- *Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.*
- *Staff should not use personal email accounts for professional purposes, especially to exchange any school related information or documents or to email parents/carers.*

- Staff should not send emails to pupils.
- Irrespectively of how staff access their school email (from home or within school), school policies still apply.
- Chain messages are not permitted or forwarded on to other school owned email addresses.

14. 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 (see section 15). 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 and staff code of conduct. 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.

15. Links with Other Policies

This Online Safety Policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour Policies
- Staff Discipline Policy
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- IT and Internet Acceptable Use Agreements
- Remote Learning Policy
- Anti-Bullying & Cyber-Bullying Policy
- Remote Learning Policy
- Induction Policy
- WSCC Code of Conduct

Appendix 1: Acceptable Use Agreement Pupils and Parents/carers

Pupil and Parent/carer Acceptable Use Policy Agreement

This is how we stay safe when we use computers:

- *I will ask a teacher or suitable adult if I want to use the computers / tablets*
- *I will only use activities that a teacher or suitable adult has told or allowed me to use*
- *I will take care of the computer and other equipment*
- *I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong*
- *I will tell a teacher or suitable adult if I see something that upsets me on the screen*
- *I will check with my teacher before I print anything*
- *I will log off or shut down a computer when I have finished using it*
- *I will keep my personal information private and not share it with anyone else*
- *I know that if I break the rules there will be a consequence*

Name of pupil

……..

Signed Pupil (at parent discretion) ……

Parent/Carer Agreement: *I agree that my child can use the school's IT 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 IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.*

Signed (parent) ……

Appendix 2: Acceptable Use Agreement Staff, Governors, Volunteers and Visitors

Name of staff member/governor/volunteer/visitor:

When using the school's IT 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 (or create, share, link to or send such material)
- 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, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- I will protect my personal devices with a pin code and a protective case.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in the online safety policy.
- I will not use personal email addresses on the school / academy IT systems, unless I have specific permission.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any loss, damage or faults involving equipment or software, however this may have happened.
- I understand that data protection policy requires that any staff or pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to governors and / or the local authority and in the event of illegal activities the involvement of the police.

I will only use the school's IT 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 and my use of the school's IT facilities and systems.* *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 SLT 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 IT 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**:
Question	**Yes/No (add comments if necessary)**
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?	