**Wolverham Primary and Nursery School**

**Online Safety Policy**

**Online Safety: The Rationale**

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

Online Safety encompasses the use of new technologies, internet (including social-networking) and electronic communications such as websites, mobile phones and video conferencing (such as Zoom/Teams/Google Meets). It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for all users to enable them to control their online experience.

**Roles and Responsibilities:**

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

The governing board will co-ordinate regular meetings with appropriate staff, usually the computing lead, to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). These take the form of reports from esafe who have identified any potential concern.

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

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

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

* 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
* Liaising with other agencies and/or external services if necessary
* Providing regular reports on online safety in school to the Governing Board and Trustees

The Online Safety Coordinators for Wolverham Primary School are **Mr Joseph Bullen and Mr Ben Grinyer** who work alongside Miss Jenni Ogden who is our Head teacher and DSL.

* The Online Safety Policy and its implementation will be reviewed annually.
* The Online Safety Policy was revised by: Ben Grinyer / Joseph Bullen

**Teaching and learning**

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*

**Internet use will enhance learning**

* The internet access will be used expressly for pupils and will include filtering appropriate to the age of pupils.
* Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation, both inside and outside of a school context.

# **Pupils will be taught how to evaluate Internet content**

* The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
* Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

**Managing Internet Access**

**Information system security**

* School ICT systems and security will be reviewed regularly with a technician on site every 2 weeks.
* Virus protection will be installed on every computer and will be set to update automatically at least every week if not daily.
* ESafe software has been installed on all school laptops and desktops and monitors inappropriate content. This company then contacts school with the risk and details of content found. If a low risk, then this is emailed weekly to SLT. If an immediate risk, then school is phoned.

**E-mail**

* Pupils will not have their own individual e-mail accounts nor will they be allowed to access any personal email addresses they have
* E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

# **Passwords**

* All computers need a password to gain access
* All passwords are kept safe
* All staff email accounts have a secure password~~,~~
* Staff USB sticks are password protected by using 64-bit encryption.
* All staff laptops have Bit Locker encryption.

# **Software**

* All software installed on computers is checked for age appropriate content, depending on the age of pupil accessing it.
* Pupils are taught about software that can be accessed outside of school, and the need for responsibility.

# **Publishing pupil’s images and work**

* Photographs that include pupils will be selected carefully and will not have children’s full names near the images.
* Pupils’ full names will not be used anywhere on the website or social media, particularly in association with photographs.
* Parents or carers will be asked to complete giving permission for their child’s photographs to be published on the school website/social media.
* An annual consent will be given to all parents/carers for the publication of children’s work and photographs on the school website/social media account.

**Social networking and personal publishing**

* The school will block/filter access to some social networking sites – these will only be used by staff in accordance with the acceptable use policy
* Pupils will be advised never to give out personal details of any kind which may identify them or their location if using social media at home.
* Staff are not allowed to post any comments on social networking sites that relate to the school and/or children/staff. All staff sign a form to agree with these terms.

**Managing filtering**

* The school will work with the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
* If staff or pupils discover an unsuitable site, it must be reported to J Bullen and B Grinyer who will take appropriate action
* Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
* eSafe software has been installed on all school laptops and desktops and monitors inappropriate content. This company then contacts school with the risk and details of content found. If a low risk, then this is emailed weekly to SLT. If an immediate risk, then school is phoned.

**Managing videoconferencing (Zoom/Microsoft Teams/Google Meets)**

* Videoconferencing with a class will only take place during lesson time and not when children are using ICT independently
* Staff must use video conferencing appropriately and report anything that could cause harm.

# **Managing emerging technologies**

* Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
* Mobile phones will not be used during lessons or formal school time.

# **Protecting personal data**

* Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and ensuring compliance with GDPR
* Children’s personal data will only be stored on teachers’ laptops that have a secure password and Bit Locker, or an encrypted USB memory stick.

# **Policy Decisions**

# **Authorising Internet access**

* All staff must read and sign the ‘Acceptable Use Policy’ before using any school ICT resource.
* All students must read and agree to the ‘Keeping Ourselves Safe Policy’ and a class charter will be signed.
* Within the school access to the Internet will be supervised. Lower down the school access will only be to specific, approved on-line materials.

**Assessing risks**

* The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
* The school will regularly audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

**Handling Online Safety complaints**

* Complaints of Internet misuse will be dealt with by a senior member of staff.
* Any complaint about staff misuse must be referred to the Headteacher.
* Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
* Pupils and parents will be informed of the complaints procedure.

**Communications Policy**

**Introducing the Online Safety policy to pupils**

* Online Safety rules will be posted in classrooms and discussed with the pupils at the start of each year.
* A ‘Keeping Ourselves Safe’ Policy is created with the Online Safety committee and reviewed each year. Every class will display this and children are made aware of the rules to stay safe and know how to report any concerns to appropriate adults in school.
* Pupils are informed that network and Internet use is monitored.
* Through the development of the Online Safety scheme of work, pupils will gain knowledge and understanding of why it is important to stay safe and how to go about this.

**Staff and the Online Safety policy**

* All staff will be given the School Online Safety Policy and its importance explained.
* Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

**Enlisting parents’ support**

* Parents’ attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school website/social media.
* 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.
* If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
* Concerns or queries about this policy can be raised with any member of staff or the headteacher.

**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.
* 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 education, and other subjects where appropriate.
* 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 anti-bullying 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.

**Examination of staff device**

Whilst the law dictates that 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, staff at Wolverham Primary school will not handle pupils’ devices without a parent present.

**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).

Volunteers will receive appropriate training and updates, if applicable.

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

Updated April 2021

Review April 2022

**Appendix 1**

Guidance in response to an incident of concern

Internet technologies and electronic communications provide children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school. However, it is also important to consider the risks associated with how these technologies are used.

Any Online Safety Policy should also recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for other users.

These risks to online safety are, of course, caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police.

This section will help staff determine what action they can take within the school and when to hand the issue over to the school-based Child Protection Co-ordinator, the Online Safety Officer or the Police Liaison Officer.

***What does electronic communication include?***

* **Internet collaboration tools:** social networking sites and blogs
* **Internet Research**: web sites, search engines and Web browsers
* **Mobile Phones and personal digital assistants** (PDAs)
* **Internet communications:** e-Mail and instant messaging (IM)
* **Webcams and videoconferencing**

***What are the risks?***

|  |  |
| --- | --- |
| * + Receiving inappropriate content   + Predation and grooming   + Requests for personal information   + Viewing ‘incitement’ sites   + Bullying and threats   + Identity theft | * + Publishing inappropriate content   + Online gambling   + Misuse of computer systems   + Publishing personal information / images   + Hacking and security breaches |

***How do we respond?***

The flowchart on the next page illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and the Child Protection Unit and Designated staff member should be consulted.

As previously stated schools should ensure that relevant policies (Acceptable Use Policy, Behaviour Policy, Bullying Policy, Discipline Policy) are referenced and are considered when dealing with the issues identified.



**A concern is raised**

Refer to school’s designated safeguarding lead

Jenni Ogden or Vicki Hughes

**Response to an Incident of Online Safety Concern**

The Screening Tool is available on the Children’s Safeguards Service site.

**School disciplinary and child protection procedures. (possible parental involvement)**

Other children involved?

**1**

**1**

**No**

**No**

**Yes**

Refer to Children’s Safeguards Service

**Possible legal action**

If appropriate, disconnect computer, seal and store.

Establish level of   
concern.

**Staff as victim**

**Child as   
instigator**

What type of   
activity is involved?

(Use screening tool)

**Illegal**

**Incident closed** (Is counselling or advice required?)

**Neither**

Who is involved?

**Inappropriate**

Establish level of   
concern.

Establish level of   
concern.

Establish level of   
concern.)

**Staff as instigator**

Counselling   
Risk assessment

**Yes**

In-school action:  
designated CP co-ordinator,   
head of ICT, senior manager.

Manage allegation procedures

Potential   
illegal or child protection  
 issues?

**Possible legal action**

**Child as   
victim**