Worsthorne Primary School

Online Safety Policy

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

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance,

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2 and it's advice for schools on:

- Preventing and tackling bullying and cyber bullying
- RSE (Relationship and Sex Education)
- Searching screening and confiscation

https://www.gov.uk/government/publications/preventing-and-tackling-bullying

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1069987/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education

https://www.gov.uk/government/publications/searching-screening-and-confiscation

It also refers to the Department's guidance on protecting children from radicalisation. https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

It reflects existing legislation, including but not limited to the Education Act 1996 https://www.legislation.gov.uk/ukpga/1996/56/contents (as amended), the Education and Inspections Act 2006 https://www.legislation.gov.uk/ukpga/2006/40/contents

and the Equality Act 2010 https://www.legislation.gov.uk/ukpga/2010/15/contents .

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.

http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

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 Mrs. Amy Angus

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.

Headteacher & Senior Leaders

Are responsible for ensuring that:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of membersof the school community. Mrs. Kayley and Mrs. Nicholls will oversee the day-to-day responsibility for online safety.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety-monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

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

Online Safety Lead (Mrs. Kayley)

Are responsible for ensuring that:

- Takes day to day responsibility for online safety issues and has a leading role in establishing andreviewing the school online safety policy
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future onlinesafety developments
- Meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering
- Attends relevant meetings with committee of Governors
- Reports regularly to Senior Leadership Team
- Incidents involving online safety, including: investigations, actions and sanctions will be the responsibility of the Online Safety Lead and the Headteacher.

Co-ordinator for Computing (Mrs. Kayley)

Responsible for ensuring that:

- 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 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 weekly 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 using 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

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- They have read and understood our social networking sites and social media policy.
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Headteacher & Online Safety Lead for investigation
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- They monitor the use of digital technologies in lessons and other school activities and implement current policies with regard to these devices
- All staff, including contractors and agency staff, and volunteers are responsible for: Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are 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

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Online-bullying
- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, Computing Lead and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged using CPOMS and dealt with appropriately in line with this policy Ensuring that any incidents of cyber-bullying are logged on CPOMS 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

Pupils:

Are responsible for:

- Knowing and understanding how to keep safe online
- Need to understand the importance of reporting abuse, misuse or access to inappropriatematerials and know how to do so
- Will be expected to know and understand the use of mobile devices and digital cameras in school. They should also know and understand the taking / use of images and on online-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents are expected to:

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

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

  What are the issues? - UK Safer Internet Centre https://saferinternet.org.uk/guide-and-resource/what-are-the-issues

  Hot topics - Childnet International

  Parent factsheet - Childnet International

  https://www.childnet.com/help-and-advice/parents-and-carers

Further information can be found on the school website or parents can speak to school directly.

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through newsletters, letters, website and information about national / local online safety literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their children's personal devices in the school
- acceptable use policy

Education – Pupils

Online safety is a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing and PHSE and is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies
- Pupils are taught in all lessons to be critically aware of the materials and content they access on-line and be guided

to validate the accuracy of information.

- Pupils are taught to acknowledge the source of information used and to respect copyright whenusing material accessed on the internet
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

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

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.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents

may underestimate how often children and young peoplecome across potentially harmful and inappropriate material on the internet and may be unsure abouthow to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website
- Parents / Carers evenings / sessions/ assemblies
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk

  www.saferinternet.org.uk

  http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff meetings/ INSET days.
- The Online Safety Lead will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training sessions, with particular importance for those who are members of any group involved in technology / online safety / health and safety/safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation
- Participation in school training / information sessions for staff or parents

Technical – equipment, filtering and monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective incarrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password. Staff are responsible for the security of their username and password and will be required to change their password every 30 days.
- The administrator passwords for the school ICT systems, used by the Network Manager must also be available to the Headteacher or other nominated senior leader.

- The School Bursar is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users.
- Daily reports are emailed to the Headteacher who checks and reports to the online safety lead when necessary.
- Internet filtering ensures that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided differentiated user-level filtering
- An appropriate system is in place for users to report any potential technical security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

Cyberbullying

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.

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 and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information 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 if it is deemed necessary to do so.

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.

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. 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.

Mobile Phones

Pupils may at times bring mobile devices into school but these must be stored in the baskets in each class which are then stored in a locked cupboard. Children are not permitted to use them during lessons, clubs before or after school, or any other activities organised by the school.

Staff using devices out of 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. No USB devices are allowed to be used within school without approval. If staff have any concerns over the security of their device, they must seek advice from the computing lead. Work devices must be used solely for work activities.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass,engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise riskof harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; dataprotection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the schoolcommunity
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of lossof personal information

Personal Use:

- Personal communications are those made via a 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 scopeof this

policy

- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitorthe Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to adefined policy or process

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of onlineservices. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. All action taken will be recorded on CPOMS under the category of Online Incident.

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.

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.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This is recorded using CPOMS and identifying the issue as an online incident. This policy will be reviewed every year by the Governors.