wfs

WyreForestSchool

Online Safety Policy

Date of last review:	2022	**Review period:**	3 Years
Date of next review:	2025	**Written by:**	Jo Kehoe
Type of policy:	Statutory	**Committee:**	Curriculum & Standards

1. Aims

Wyre Forest 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 all forms of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, including but not limited to pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes harm, such as making, sending and receiving explicit images (e.g. sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

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***

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***, 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 and our systems also take into account the guidance of the UK Safer Internet Centre and its guidance document *Appropriate Filtering for Education Settings.*

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 discuss any key online safety issues, as part of their monitoring discussions with the designated safeguarding lead (DSL) and the deputy headteacher - safeguarding and families (DHT- SF).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms of acceptable use of the school's ICT systems and the internet

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 & deputy headteacher safeguarding & families

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy

The DSL, DHT-SF and the IT & Technical Support Manager take the 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 and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school safeguarding policy
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school safeguarding policy.
- Updating and delivering staff training on online safety, as part of wider whole school safeguarding training
- Liaising with other agencies and/or external services if necessary.

3.4 The IT & technical support manager

The IT & technical support manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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.
- Ensuring updates that are available to servers and systems are checked and installed every half-term, or immediately in the event of a critical update release.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

3.5 All staff and volunteers

All staff and volunteers are responsible for:

- Maintaining an understanding of the key aspects of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms of 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 & DHT-SF to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school safeguarding policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

3.6 Parents/Carers

Parents/Carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Support their child in understanding the importance of online safety and report any incidents of concern with the class teacher.

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

- What are the issues? ***UK Safer Internet Centre***
- Hot topics; ***Childnet International***
- Parent resource sheets; ***Childnet International***
- Parent guides; thinkuknowhow.co.uk
- Setting up parental controls; Parental Controls & Privacy Setting Guides internetmatters.org
- Healthy relationships: disrespectnobody.co.uk

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.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. This will be through key learning from the WFS Progression Steps and where appropriate the National Curriculum:

The text below is taken from the ***National Curriculum computing programmes of study.***

It is also taken from the ***guidance on relationships education, relationships and sex education (RSE) and health education.***

At WFS we teach pupils the skills of online safety and RSE, in line with the pupils' levels of understanding. The curriculum is planned in line with the expectations that all schools have to teach, including those of:

- ***Relationships education and health education*** for primary age pupils.
- ***Relationships and sex education and health education*** for secondary age pupils.

Expectations for pupils of Key Stage 1 age are that 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.
- Expectations for pupils of Key Stage 2 age are that pupils 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.

Expectations are that by the end of Key Stage 2 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.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Expectations for pupils of Key Stage 3 age are that pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Expectations for pupils of Key Stage 4 age are that pupils will be taught to:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

Expectations are that by the end of Key Stage 4 pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

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

5. Educating parents/carers about online safety

The school will raise parents'/carers' awareness of internet safety in letters or other communications home, and in information via our website, newsletters and workshops. 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 class teacher.

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

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 also the school behaviour and the safeguarding policies.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will use our best endeavours to 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. We will support pupils to understand this at their own level. Also, school IT systems are configured to minimise exposure to external risks and include logging and reporting on user activity for safeguarding purposes.

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 as part of the curriculum. Teaching staff will also find opportunities to use aspects of the curriculum to cover cyber-bullying.

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 safeguarding 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 & DHT-SF 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.
- disrupt teaching.
- break any of the school rules.

Unless a safeguarding issue, decisions regarding this will always be made in discussion with parents or carers.

If inappropriate material is found on the device, it is up to the DSL or DHT-SF to decide whether they should:

- delete that material.
- retain it as evidence (of a criminal offence or a breach of school discipline).
- report it to the police.

The DSL or DHT-SF may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE’s latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school’s Searching, Screening & Confiscation Policy

After an incident, the pupils will be supported in further developing their understanding of the significance of the event.

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 visitors will be required to read and agree to the school’s terms on acceptable use before being granted access to the schools’ IT systems or allowed access to the internet via the schools’ network.

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 and activity of pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

8. Pupils using mobile devices in school

The appropriate and acceptable use of mobile devices by pupils is set out in the WFS Pupils Mobile Phones & Devices Policy

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour and safeguarding policies, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their work-issued 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).
- Not sharing the device among family, friends or other colleagues, unless the device is specifically set up for this purpose.
- Looking after any devices by keeping them in a secure location and in a protective case when not in use.

Staff members must not use the device in any way which would violate the school’s terms of acceptable use.

Work devices must be used solely for work activities. School monitoring systems are still active on devices when used outside the school.

If staff have any concerns over the security of their device, they must seek advice from the IT & technical support manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school’s ICT systems or internet, we will follow the procedures set out in our policies. 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 staff disciplinary procedures and the 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.

11. 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., as part of the safeguarding training.

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).

By way of this training, all staff will be made aware that:

- Pupils with special educational needs and disabilities (SEND) are particularly vulnerable to this form of abuse.
- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages.
    - Sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
    - Sharing of abusive images and pornography.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training and the ongoing curriculum will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse.
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up.
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

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.

12. Monitoring arrangements

All online safety related concerns are recorded on CPOMs. The safeguarding team will monitor levels of incidents and respond accordingly.

This policy will be reviewed every three years by the Deputy Headteacher – Teaching, Learning & Curriculum (DHT-TLC). At every review, the policy will be shared with the governing body, all staff and parents/carers.

13. Links with other policies

This online safety policy is linked to our:

Safeguarding policy, including child protection

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

ICT and internet acceptable use policy

Pupil Mobile Phones & Devices Policy

Searching, Screening & Confiscation Policy