



Online Safety Policy

Approved/reviewed by	
WSL SLT team	
Date adopted:	April 2020
Date of review	September 2021
Date of next review	September 2022

This policy is reviewed annually to ensure compliance with current regulations

Contents

1. Aims.....	3
2. Legislation and guidance	3
3. Roles and responsibilities.....	4
3.1 The governing board	4
3.2 The Head of Centre	4
3.3 The designated safeguarding lead.....	4
3.4 The Administrator Lead	5
3.5 All staff and volunteers	6
3.6 Parents.....	6
3.7 Visitors and members of the community	6
4. Educating pupils about online safety	7
5. Educating parents about online safety.....	8
6. Cyber-bullying.....	9
6.1 Definition	9
6.2 Preventing and addressing cyber-bullying	9
6.3 Examining electronic devices.....	10
7. Acceptable use of the internet in school.....	11
8. Pupils using mobile devices in school	11
9. Staff using work devices outside WSL.....	11
10. How the school will respond to issues of misuse	12
11. Training.....	12
12. Monitoring arrangements	13
13. Links with other policies	13
Appendix 1: WSL acceptable use agreement (pupils and parents/carers).....	14
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors).....	15
Appendix 3: online safety training needs – self audit for staff	16
Appendix 4: online safety incident report log.....	17

1. Aims

WSL 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 Head Teachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The governing board

The SLT team has overall responsibility for monitoring this policy and holding the Head of Centre to account for its implementation.

The Head of Centre will report to the SLT team and coordinate meetings with staff to discuss online safety, and monitor online safety logs as provided by the WSL.

The SLT team 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 3)

3.2 The Head of Centre

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

3.3 The designated safeguarding lead

Details of the WSL's DSL are set out in our child protection and safeguarding policy as well relevant job descriptions.

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

- Supporting the Head of Centre/ Director of Education/Proprietor in ensuring that staff understand this policy and that it is being implemented consistently throughout the WSL.
- Working with the HoC, SLT team, Senior staff, the Admin lead and other staff, as necessary, to address any online safety issues or incidents

- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the WSL behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the HoC and/or SLT team
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the WSL behaviour policy

This list is not intended to be exhaustive.

3.4 The Administrator Lead

The Administrator Lead 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 ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly and identify external support where needed
- Conducting a full security check and monitoring the WSL's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Identify and ensure that any online safety incidents are logged (see appendix 4) and are reported to the DSL

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 ICT systems and the internet (appendix 3), and ensuring that pupils follow the WSL's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are reported and check that it has been followed up appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Head of Centre 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 (appendices 1 and 2)

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](#)

3.7 Visitors and members of the community

Visitors and members of the community are encouraged to bring their own resources e.g. when delivering training. Where the WSL's ICT system or internet is

needed, members and visitors 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 3).

4. Educating pupils about online safety

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

From September 2020 all schools will have to teach:

Relationships and sex education and health education in secondary schools

This new requirement includes aspects about online safety.

In **Key Stage 3**, 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

Pupils in **Key Stage 4/5** will be taught:

- 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

*By the **end of secondary school**, they 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*

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

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

5. Educating parents about online safety

WSL will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents.

Online safety will also be covered during parents' WSL events.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of Centre/DSL.

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

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 policy.)

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.

WSL will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Key staff such as PSHE teachers will discuss cyber-bullying with their pupils, and the issue will be addressed in assemblies and debrief sessions.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

WSL 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 WSL 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.

6.3 Examining electronic devices

WSL 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 WSL complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the WSL's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the WSL's terms on acceptable use if relevant.

Use of the WSL'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 and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into WSL, but are not permitted to use them during:

- The school day unless they have been given permission to do so by a member of staff
- Clubs before or after school, or any other activities organised by WSL

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

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

9. Staff using work devices outside WSL

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

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

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

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the WSL's ICT systems or internet, we will follow the procedures set out in our policies on behaviour management. 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 WSL'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/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

WSL 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.

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 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.

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

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

This policy will be reviewed every year by the Head of Centre. At every review, the policy will be shared with the SLT team.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

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

ACCEPTABLE USE OF WSL ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
<p>I will read and follow the rules in the acceptable use agreement policy When I use the WSL's ICT systems (like computers) and get onto the internet in WSL I will:</p> <ul style="list-style-type: none"> • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it <p>I will not:</p> <ul style="list-style-type: none"> • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision <p>If I bring a personal mobile phone or other personal electronic device into school:</p> <ul style="list-style-type: none"> • I will not use it during lessons, debrief time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online <p>I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.</p>	
Signed (pupil):	Date:
<p>Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.</p>	
Signed (parent/carer):	Date:

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

ACCEPTABLE USE OF THE WSL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
<p>When using the WSL's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:</p> <ul style="list-style-type: none"> • 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 WSL'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 WSL's network • Share my password with others or log in to the WSL's network using someone else's details • Take photographs of pupils without checking with HOC & DOC • Share confidential information about the WSL, 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 	
<p>I will only use the WSL's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.</p> <p>I agree that the school will monitor the websites I visit and my use of the WSL's ICT facilities and systems.</p> <p>I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside WSL, and keep all data securely stored in accordance with this policy and the school's data protection policy.</p> <p>I will let the designated safeguarding lead (DSL) and Admin Lead 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.</p> <p>I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.</p>	
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?	

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG			
Date		Where the incident took place	
Description of the incident			
Action taken			
Staff member recording the incident			