West SILC

Online Safety

& Acceptable Use Policy

The 4 Cs of online safety: content, contact, conduct and commerce

Content: seeing illegal, inappropriate or harmful content

Contact: harmful interactions

Conduct: behaviour that increases the chances of, or causes, harm

Commerce: gambling, advertising, scams

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 statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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.

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

3. Roles and responsibilities

3.1 The governing board

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

The governing board 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).

On line safety is overseen by 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 Principal

The Principal (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 designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

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

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Collaborating with the IT technician to ensure the efficiency of filtering and monitoring systems, which includes conducting checks on both systems.
- 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 school 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 Principal and governing board

3.4 The ICT technician

The ICT manager 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
- Report all filtering and monitoring incidents to the DSL (Designated Safeguarding Lead) through Behaviour Watch when learners are directly impacted and via email when they are not
- 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 that are logged 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 following the direction of 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 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 (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 school behaviour policy
- Comply with all areas of the SILC's Acceptable Use Agreement that relate to their use
- Report any cause for concern when a learner is exposed to inappropriate material, whether impacted or not. Additionally, send an email to the DSL (Designated Safeguarding Lead) when a learner is not impacted but encounters inappropriate material that is not prevented by the SILC's monitoring and filtering arrangements.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Principal 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 where this is appropriate for the child (appendix 1)
- Comply with all areas of the SILCS' Acceptable Use Agreement that relate to them

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://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

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. If appropriate, they will be expected to agree to the terms on acceptable use agreement (appendix 2).

4. Educating pupils about online safety

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

As appropriate, with sensitivity to our pupils' cognitive development, 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

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- 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
- 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
- They will be aware of the risks from the 4 Cs of online safety
    - Content
    - Contact
    - Conduct
    - Contract

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

The school will use assemblies, focused weeks and special events 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

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.

Online safety will also be covered during parents' evenings, including information around the sharing of nudes and semi nudes when required.

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

However, concerns or queries about this policy can be raised with any member of staff in the first instance.

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 anti-bullying policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils are supported to understand what it is and what to do if they become aware of it happening to them or others.

Where applicable, 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. Staff will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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, 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/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 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

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.

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 school's ICT systems and the internet (appendices 1 and 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.

8. Pupils using mobile devices in school

Pupils are discouraged from bringing mobile devices to school. However, we recognise there may be occasions, for example where pupils are independent travellers, that pupils may have a legitimate need to have access to a mobile device.

Pupils may bring mobile devices into school, but are not permitted to use them during the school day and they should be handed in for safe keeping on arrival. Pupils will be allowed access to their mobile device during educational visits that extend beyond the normal school day. The school accepts no responsibility or liability for damage or loss to any mobile deceives brought to school.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

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 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, as set out in appendix 2.

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

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

Work devices must be used solely for work activities.

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 the behaviour policy. 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 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.

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 3 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.

12. Monitoring arrangements

Staff will log behaviour and safeguarding issues related to online safety. This will be done using the Behaviour Watch system (Cause for Concern) or via email to the DSL if no learner/s have been impacted.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the governing board.

13. Links with other policies

This policy will be approved by the SILC's Governing Body

This policy should be read in conjunction with

Equality ACT 2010

West SILC Teaching and Learning Policy

West SILC Behaviour Policy

West SILC Anti Bullying Policy

West SILC Safeguarding and Child Protection Policy (and relevant addendums)

John Mace, Vice Principal - September 2023

Review date September 2024

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

West SILC: Acceptable use of the school's ICT systems and remote learning platforms and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in or out of school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms (unless my teacher has expressly allowed this as part of a learning activity and is full supervised)
- Open any attachments in emails from unfamiliar sources, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

When accessing remote learning, I will:

- Not to make recordings of a live lesson or interaction without express written permission from the relevant member of staff
- Not store or distribute any recordings of live lessons that have been made
- Not redistribute links to live sessions or recordings
- Join live sessions at the time requested/scheduled by the member of staff
- Ensure I am appropriately dressed in case the camera is switched on mistakenly
- Be in a suitable space for learning, wherever possible. I should be able to hear and give the lesson my full attention.
- Always be muted unless a member of staff asks me to speak, to avoid people talking over one another
- Ensure I have appropriate learning materials for the lesson if appropriate, with support if needed
- Be ready to contribute and fully engage in the learning
- Behave appropriately and with respect to others
- Only post appropriate comments related to the learning in the chat

If I bring a personal mobile device into school:

- I will not use it during lessons, tutor group 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
- Only use the device in conjunction with the guidance in all other SILC policies

I agree that the school will monitor the websites I visit.

I will immediately let a member of staff or trusted adult know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

Signed (pupil): *Parents may sign on a pupil's behalf.*	**Date:**

Parent/carer 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. I agree that, for remote learning, I have responsibility for monitoring the safety of the pupil. Furthermore, I agree to:

- Support the pupil to access the lessons. *For example, checking your child can log in to Office 365 and Microsoft Teams*
- Parents/carers should ensure adequate supervision of all activities including live sessions
- Ensure, as noted above, their pupil is joining live lessons dressed appropriately

- Ensure the pupil has a suitable space to work in, wherever possible, so that the pupil can hear and engage fully in the lesson
- Check-in with their child's learning by asking them about the live lessons and engaging in conversations with them about these
- Let school know if their child is having difficulties or needs some support accessing the live lessons
- Support school in maintaining high standards of behaviour wherever possible, encouraging their child to avoid interrupting others or posting inappropriate comments in the chat. *High standards of behaviour are still expected for remote learning.*
- Not redistribute links to live lessons or recordings
- As noted above, we may record some of the live sessions to make them available for other members of the class at a more flexible time. Again, these sessions must not be stored or distributed by yourself. By allowing the pupil to participate in a live lessons you are giving permission for this to take place. The member of staff will make it known at the beginning of the session, whether it is to be recorded. *Where the school finds that a parent/carer has distributed a recording action will be taken.*

Signed (parent/carer):	**Date:**

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

West SILC: Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT 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
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms for non-work related purposes
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details
- Schedule 1:1s, groups only. In cases where 1:1 tuition is deemed essential, staff must seek formal written agreement from a member of the Senior Leadership Team and the pupil's parent / carer. A recording of all remote learning should be made where a supervising second is not present.

When taking part in or delivering remote learning I will:

- When the technology allows, schedule live lessons as 'meetings' ensuring 'meeting options' are appropriate e.g. users can not bypass the lobby.
- Manage participation of pupils.
- Be appropriately attired and in a suitable location.
- Check the participant list for 'live' lesson. Keep a record of who attended your lesson.
- Be mindful of professionalism and ensure that they keep language/dialogue appropriate as if teaching in a classroom.
- Group calls should have two members of staff in them, wherever possible. The preference for 1:1 session is for them to take place in school. If this is not achievable then another member of staff needs to be present (this can be virtually). Again, if this is not achievable then the session can go ahead with prior, written, agreement from a member of the Senior Leadership Team **and** the parent/carer. A recording of these sessions should be made.
- Let participants know if a live session is being recorded.

I will only use the school'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.

I agree that the school will monitor the websites I visit.

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 ICT technician 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. Any deficiencies in the reporting and monitoring procedures will be brought to the attention of the DSL

I will always use the school's ICT 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:**
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? Please record them here.	

Appendix 4: online safety incident report log to be used where Behaviour Watch or emails are unavailable

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**