Online Safety Policy
Sherdley Primary School

Approved by:	**Date:** October 2022
Last reviewed on:	
Next review due by:	

The Key

Approved by forbessolicitors.

Contents

1. Aims....2
2. Legislation and guidance....3
3. Roles and responsibilities....3
4. Educating pupils about online safety....5
5. Educating parents about online safety....5
6. Cyber-bullying....6
7. Acceptable use of the internet in school....7
8. Pupils using mobile devices in school....7
9. Staff using work devices outside school....8
10. How the school will respond to issues of misuse....8
11. Training....8
12. Monitoring arrangements....9
13. Links with other policies....9
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)....**Error! Bookmark not defined.**
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)**Error! Bookmark not defined.**
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)....**Error! Bookmark not defined.**
Appendix 4: online safety training needs – self-audit for staff....13
Appendix 5: Online Safety Curriculum Overview 14

---

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, including mobile and smart technology (which we refer to as 'mobile phones')
- 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, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as child-on-child 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., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **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's) 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 (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 headteacher 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).

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 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

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

Details of the school's designated safeguarding lead (DSL), and deputies, are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes 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, ICT manager (the local authority) 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 child protection policy
- Ensuring that any online safety incidents are logged/recorded on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged/recorded 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
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT (The Local Authority) manager

The local authority provides all IT services, which include: IT support, advice, firewalls, filtering, technical support, wi-fi and networks and all back-up services. The ICT 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
- 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 monitored via Smoothwall 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

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 school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL 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 behaviour 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'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff in line with our school graduated approach, member of the senior leadership team 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 (appendices 1 and 2)
- Play an active role in monitoring and safeguarding their children's online activity outside of school

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 resource sheet – Childnet International

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 (appendix 3).

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools

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
- 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

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in newsletters, via the school app, and in information via our website. This policy will also be shared with parents.

The school will let parents know:

- What systems the school uses to filter and monitor online use – the local authority provide robust filtering systems, monitoring is done via Smoothwall

- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

We would encourage parents to apply filters to devices that children can access at home or I the community.

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

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

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 1 person or group by another person or group, where the relationship involves an imbalance of power.

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 educate pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim as well as if they are a victim.

The school will actively discuss cyber-bullying and e-safety at the start of each term 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/e-safety with their classes during computing lessons, or if /when a need arises.

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, as well as weekly Paws for Thought class assemblies where issues pertinent to specific classes can be addressed promptly.

All staff, governors 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).

The school also shares 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. These can also be found on the school website, on the E-Safety page.

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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (the Deputy and Assistant Headteachers) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- Inform parents/carers and wherever possible wait for them to be in attendance before carrying out a search
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation, use an appropriate space for the privacy and dignity of the pupil being searched, and have an appropriate additional adult present (wherever possible the pupils' parents/carers)

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL and/or Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, appointed staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL/Headteacher immediately, who will decide what to do next. The DSL/Headteacher will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

Being part of Sherdley Primary School means that all pupils, parents, staff, volunteers and governors will agree, and give regard to the schools Acceptable Use Agreements, including the use of the internet and the school's ICT systems and equipment. 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. The local authority IT service supports school with the appropriate systems.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

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

- Lessons
- Break or lunchtimes
- Clubs before or after school, or any other activities organised by the school

Device should be given to class teachers to store during the school day.

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 school

All staff members will take appropriate steps to ensure their 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)
- Store work on the school's Office 365 Cloud, as this is monitored and backed up by the local authority
- Ensuring that no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

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

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 on behaviour and online safety, including ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate in line with our school graduated approach.

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 code of conduct policy. 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 and staff meetings).

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

- 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
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training 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 up the risks
- 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 deputy DSLs 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.

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

12. Monitoring arrangements

All staff log behaviour and safeguarding issues related to online safety. All records on CPOMS will be monitored, reviewed and actioned by the DSL and DDSLs as part of regular Safeguarding supervision meetings.

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

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding & Child Protection Policy
- Behaviour Policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- GDPR Policies
- Computing Curriculum Policy
- SEND Policy
- PSHE Policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

When I use the school devices (like computers, tablets and IPads) I must help keep me and other people safe.

- I will ask a teacher or adult if I want to use the computers/tablets.
- I will only look at website pages, APPs, games and videos that a teacher or adult has told me I am allowed to use.
- I will take care of the computers/tablets and tell a teacher or adult straight away if something is broken or not working.
- I will tell my teacher or a trusted adult straight away if:
    - I click on a website by mistake
    - I get sent a message from people I don't know
    - Anything 'pops up' on my screen that shouldn't be there
    - I find anything that may upset, scare or harm me or my friends
- Use school computers for school-work only
- Be kind to others and not upset, be mean or be rude to them
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules and expectations.

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

When I use devices, I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and passwords safe and secure and not share them with anyone else.
- I will not share personal information about myself or others when online.
- I will be aware of 'stranger danger' when I am online and if I arrange to meet people off-line that I have communicated with online, I will do so in a public place, taking a trusted adult with me, and having taken every possible precaution to ensure my own safety (informing trusted adults/parents/carers, sharing online discussions, making in person phone calls on a speaker phone with a trusted adult present etc)
- I will immediately tell an adult if I see anything that makes me feel uncomfortable, or that I feel may make others feel uncomfortable, when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any device or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do; as part of my Computing lessons, or that I have permission from an adult for (e.g. I will not access social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity)

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act towards me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.
- I will not add other people to groups without their permission.

I know that there are other rules that I need to follow:

- I will only use my own personal devices (including phone) in the school if I have permission, and will use it responsibly – not accessing any inappropriate websites or other inappropriate material, and I will not use inappropriate language when communicating online.
- I will only use social media sites with permission and at the times that are allowed.
- Where work is Copyright, I will not try to download copies (including music and videos), and I should have permission if I use the original work of others in my own work.
- When I am using the internet to find information, I will take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I will not open attachments, or follow links, in emails without first checking with a trusted adult.
- I will not create, link to or post any material that is offensive, rude, pornographic or otherwise inappropriate.

I understand that I am responsible for MY actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary actions – this means consequences and it may include recording on Trackit-Lights and Reflection, contacting my parents and in the event of illegal activities may involve contacting the police.

I agree that I will abide by these school expectations, and will be responsible for my out of school online behaviour.

Appendix 3: acceptable use agreement

(staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • 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 school'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 school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, 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
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 and my use of the school's ICT facilities and systems. 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 manager know if a pupil informs you that 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. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. I will only use my personal mobile phone or device in offices, staffrooms or areas away from children. I will NOT share school based information on any of my personal social media platforms.

NB - Staff, governors, volunteers and visitors will not be given access to the school Wi-Fi for their own personal devices. Personal devices, such as mobile phones, MUST NOT be used in classrooms or around children; these can be used in staffrooms and office areas.

Appendix 4: online safety training needs – self-audit for staff

Adapt this form to suit your needs.

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?	
Are you aware of the ways pupils can abuse their peers online?	
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?	

Planning e-Safety Across the School

This grid outlines a range of online safety lessons and activities that can be planned by each year group across the year. We recommend that teachers deliver at least one online safety activity each half term. Often, we have planned more than one activity in a half term. This enables the teacher to develop or reinforce learning if they feel this would be beneficial. The order of the activities can also be changed if you think your pupils will benefit from a particular theme earlier in the year.

All the activities are freely available online. Most ask for the teacher to login and register an account to download the full resources. This allows the e-safety organisation to track how many schools are using their resources and monitor their effectiveness. Often, you can log in with your school Google or Microsoft account.

Please download resources before the lesson and tailor them to the needs of your class. You may find you do not need to use all of the suggested activities, or you can adapt an activity to better suit your class.

Underneath the activities for each year group are the skills from hi-impact's key skills curriculum mapping. This ensures that each year group has a set of skills to move them forward each year in learning about e-safety.

Links to the 8 themes of Education for a Connected World framework are made at the bottom of the Common Sense Media Lessons. Education for a Connected World was based on the themes of Commonsense Media.

Education for a Connected World **Common Sense Education**

- Self Image & Identity ---------- Media Balance & Well-Being
- Online Relationships ---------- Relationships & Communication
- Online Reputation ---------- Relationships & Communication
- Online Bullying ---------- Cyberbullying, Digital Drama & Hate Speech
- Managing Online Information ---------- News & Media Literacy
- Health, Wellbeing and Lifestyle -------- Media Balance & Well-Being
- Privacy and Security ---------- Privacy & Security
- Copyright and ownership ---------- News & Media Literacy

Commonsense Media lessons have a UK-focused version.

Further support can also be found at Project Evolve, a repository of resources to support this EfCW, **Please note - do not use Project Evolve as a scheme.** It is not designed for this. Rather, to supplement and consolidate what is already planned. Please ask for advice from hi-impact

Year 1			
Online Communication	**Activity 1** **Introduction** What online experiences do the class already have? **DL1.5** **EfCW** • Online Relationships • Managing Online Information **Activity 2** Jessie and friends - Watching videos **DL1.5** **EfCW** • Managing online information • Self-Image and Identity	**Activity 1** Media Balance Is Important **DL1.5** **EfCW** • Managing online information • Self-image and identity • Online Bullying • Health, well-being and lifestyle **Activity 2** Use the school VLE (virtual learning environment). **DL1.1, DL1.2** **EfCW** • Privacy and Security • Managing online information • Online Relationships • Online Reputation • Copyright and Ownership	**Activity 1** Safety in My Online Neighbourhood. **DL1.5** **EfCW** • Managing online information • Privacy and Security **Activity 2** Pause for People **DL1.5** **EfCW** • Health, well-being and lifestyle • Self-Image and Identity
Key Skills	• **DL1.5** Be aware of some of the dangers of online activity and know to tell an adult if they feel something they see online is inappropriate or hurtful. • **DL1.2** With support, be able to access and view pictures or work via an online platform		

Year 2	Ongoing. When producing digital content on a tablet or PC, upload the content to a digital platform to which the school utilises e.g. Google Classroom, Teams, eSchools, Seesaw, Tiny Tap, Buncee etc. **DL2.2** *To access the **Common Sense Media** materials you will need to create a teacher account. You will then be able to access and download all the teacher and pupil resources for each lesson.*					
Online Communication	School rules for staying safe online. **DL2.5** **EfCW** • Online relationships • Health, wellbeing and lifestyle • Managing information online	Jessie and Friends Dangers of sharing photographs they take with a phone or tablet. **DL2.5** **EfCW** • Online reputation • Privacy and security • Copyright and Ownership • Managing Online Information	Jessie and Friends Keep personal information private, **DL2.5** **EfCW** • Online relationships • Health, wellbeing and lifestyle • Privacy and security • Self-Image and Identity • Online Bullying	Pause and think Online - **DL2.5** **EfCW** • Online relationships • Health, wellbeing and lifestyle	Internet Traffic Lights. **DL2.5** **EfCW** • Health, wellbeing and lifestyle	How technology makes you feel? **DL2.5** **EfCW** • Health, wellbeing and lifestyle
Key Skills	**DL2.2** With support, be able to share pictures or work to an online platform. **DL2.5** Be able to explain online danger and begin to be responsible for their actions online including saying what personal information should be kept private and explain why it is important to discuss their use of technology with an adult.					

Year 3	Ongoing. When producing digital content on a tablet or PC, upload the content to a digital platform to which the school utilises e.g. Google Classroom, Teams, eSchools, Seesaw, Tiny Tap, Buncee etc. **DL2.2** *To access the **Common Sense Media** materials you will need to create a teacher account. You will then be able to access and download all the teacher and pupil resources for each lesson. See the tutorial here.*					
	Common Sense Materials Device-Free Moments **DL3.5** **EfCW** • Health, wellbeing and lifestyle	**Common Sense Materials** That's Private! **DL3.5** **EfCW** • Privacy and security .	**Common Sense Materials** Digital Trails **DL3.5** **EfCW** • Privacy and security • Online reputation • Managing information online	**Common Sense Materials** Who Is in Your Online Community? **DL3.5** **EfCW** • Self-image and identity • Online relationships • Online reputation • Online bullying	**Common Sense Materials** Putting a STOP to Online Meanness **DL3.5** **EfCW** • Self-image and identity • Online relationships • Online reputation • Online bullying	**Common Sense Materials** Let's Give Credit! **DL3.5** **EfCW** • Copyright and ownership
Key Skills	• **DL3.2** Be able to independently share suitable pictures and work on an online platform. • **DL3.5** Be aware of some of the consequences of their online actions and be able to explain the importance of balancing game and screen time with other parts of their lives.					

Year 4	*To access the **Common Sense Media** materials you will need to create a teacher account. You will then be able to access and download all the teacher and pupil resources for each lesson.*					
Online Communication	Password powerup **DL4.5** **EfCW** • Privacy and security	Rings of Responsibility **DL4.6** **EfCW** • Online relationships	This is me - Online **DL4.6** **EfCW** • Online relationships • Self-image and identity • Online Reputation	Our Digital Citizenship Pledge **DL4.6** **EfCW** • Online relationships • Self-image and identity • Health, well-being and lifestyle • Copyright and Ownership	The Power of Words **DL4.6** **EfCW** • Online relationships • Online bullying	Seeing is believing **DL4.1** **EfCW** • Self-image and identity • Managing Online Information • Copyright and Ownership
Key Skills	**DL4.1** When searching for information online, be able to evaluate how appropriate a website is. **DL4.5** Be able to understand the reasons for using strong passwords. **DL4.6** Be aware of ways in which we interact with online communities and be able to suggest and use strategies for dealing with cyberbullying.					

Year 5	*To access the **Common Sense Media** materials you will need to create a teacher account. You will then be able to access and download all the teacher and pupil resources for each lesson.* **Ongoing - School VLE** (Virtual Learning Environment) e.g. Google Classroom, Teams, eSchools or Seesaw for pupils to upload and download content to a digital platform. **DL5.2**
Online Communication	**Extension Activities - Band Runner** Explore the Band Runner story and activities from Think U Know. Watch the Play Like Share episodes and discuss the issues the children face and how they react to issues they face online. Allow children the chance to play the band runner game featuring characters and safety messages from the Thinkuknow Play Like Share films, Band Runner is a fun game that will put children's knowledge about online safety to the test by asking them to help characters make safe choices. **DL5.5** **EfCW** ● Online reputations ● Self-image and identity ● Online bullying ● Health, wellbeing and lifestyle **Digital Compass website** Use the Digital Compass game to explore a number of common eSafety issues that pupils will likely encounter in their use of the internet at home and in school. Each group could complete a character's journey and report back what they have learnt about Dos and Don'ts to keep safe online. Pupils could then explore the other activities on the page. Educator's guide **DL5.5** **EfCW** ● Online reputations ● Self-image and identity ● Health, wellbeing and lifestyle
	Core Activities

	Private and personal Information **DL5.5** **EfCW** • Managing online information • Privacy and Security	Digital Citizenship - **DL5.5, DL6.6** **EfCW** • Online relationships • Health, wellbeing and lifestyle • Online Bullying	My Media Choices - **DL5.5, DL5.6** **EfCW** • Self-image and identity • Health, wellbeing and lifestyle	A Creator's Rights and Responsibilities **DL5.5** **EfCW** • Self-image and identity • Health, wellbeing and lifestyle • Copyright and Ownership	Keeping game fun and healthy **DL5.6** **EfCW** • Online relationships • Health, wellbeing and lifestyle • Online Bullying	Online Tracks **DL5.5** **EfCW** • Online reputations • Managing online information • Health, wellbeing and lifestyle
Key Skills	• **DL5.5** Be able to demonstrate an understanding of responsible social media use, including knowledge of their digital footprint, sharing information and images, and communication with others. • **DL5.6** Be able to demonstrate an understanding of the risks of online gaming and know strategies for healthy online behaviours.					

<table>
<tr><td>Year 6</td><td colspan="6">To access the Common Sense Media materials you will need to create a teacher account. You will then be able to access and download all the teacher and pupil resources for each lesson.

Ongoing - School VLE (Virtual Learning Environment)
E.g. Google Classroom, Teams, eSchools, Seesaw etc. for pupils to upload and download content to a digital platform.
DL6.4
EfCW
● Managing online</td></tr>
<tr><td></td><td>Media balance
DL6.6
EfCW
● Health, wellbeing and lifestyle</td><td>You Won't Believe this!
DL6.5
EfCW
● Health, wellbeing and lifestyle
● Managing online information
● Privacy and Security</td><td>Beyond Gender Stereotypes
DL6.5
EfCW
● Self-image and identity
● Online relationships</td><td>Digital Friendship
DL6.6
EfCW
● Self-image and identity
● Online relationships
● Online bullying
● Online reputation</td><td>Cyber bullying
DL6.6
EfCW
● Online bullying</td><td>Reading the News
DL6.5
EfCW
● Managing online information
● Health, wellbeing and lifestyle
● Privacy and Security
● Copyright and Ownership</td></tr>
<tr><td></td><td colspan="6">Extension
Digital Compass website.
Use the Digital Compass game to explore a number of common eSafety issues that pupils will likely encounter in their use of the internet at home and in school. Each group could complete a character's journey and report back what they have learnt about 'Dos and Don'ts' to keep safe online. Pupils could then explore the other activities on the page. Educator's guide NOTE: Check if this has been used previously and if so, what was covered in Y5.
DL6.5
EfCW
● Online reputations
● Self-image and identity
● Health, wellbeing and lifestyle

Use the Be Internet Awesome with Google website to find resources, lesson ideas and allow the children to play the online game</td></tr>
</table>

	'Interland'. This game touches on some of the key e-safety concepts of being a good digital citizen. Resource Page Curriculum links document					
Online Communication Option 2	**Be Internet Awesome** Theme 1: Share with Care - Use Protecting yourself and your reputation **DL6.6** **EfCW** • Online reputation • Privacy and security	**Be Internet Awesome** Theme 2: Don't fall for Fake - Can we believe all we read? Be Internet Awesome **DL6.1** **EfCW** • Managing online information • Health, wellbeing and lifestyle	**Be Internet Awesome** Theme 4: From Bystanders to Upstanders Students practice identifying the four roles of a bullying encounter (the person who bullies, the target of the bullying, the bystander, and the upstander) and what to do if they're a bystander or a target of bullying. Be Internet Awesome **DL6.6** **EfCW** • Online relationships • Online bullying	**Be Internet Awesome** Theme 5: When in Doubt, Talk It Out Defining and encouraging responsible internet behaviour. Be Internet Awesome **DL6.6** **EfCW** • Online relationships		
Key Skills	**DL6.1** Be able to identify irrelevant, implausible and inappropriate information when searching for information online. **DL6.5** Be able to demonstrate an understanding of media bias and strategies for ensuring a balanced view, including gender stereotypes. **DL6.6** Be able to explain how to develop positive online relationships and have strategies to prevent and stop negative situations and manage their private information.					

Appendix A9 from Online Safety Policy

A9 Responding to incidents of misuse – flow chart