



Online Safety Policy

Approved on:	19/05/2025
FGB/Committee:	FGB
Responsibility:	Headteacher
Review Date:	May 2028
Signed by Headteacher:	
Signed by Chair of Governors:	

Contents

1. Aims	0
2. Legislation and guidance	1
3. Roles and responsibilities	1
4. Educating pupils about online safety	4
5. Educating parents/carers about online safety	5
6. Cyber-bullying	5
7. Acceptable use of the internet in school	6
8. Pupils using mobile devices in school.....	7
9. Staff using work devices outside school	7
10. How the school will respond to issues of misuse.....	7
11. Training	8
12. Monitoring arrangements	8
13. Links with other policies	8
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	Error! Bookmark not defined.
Appendix 5: online safety incident report log	Error! Bookmark not defined.

1. 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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 peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. 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. 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. 3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Governing Body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Governing Body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Governing Body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the [DfE's filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure 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 (DSL, DDSL)

Details of the school's designated safeguarding lead (DSL) and deputy DSLs (DDSL) 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:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Governing Body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the School Business Manager (SBM) to make sure the appropriate systems and processes are in place
- Working with the SBM 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's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged (see appendix 5) 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 4 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 Governing Body
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The School Business Manager

The School Business Manager is responsible for the following:-

- Ensuring an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, are in place and are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensuring full security check and monitoring the school's ICT systems on a regular basis by the school's IT support provider.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) 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, and ensuring that pupils follow the school's terms on acceptable use (appendix B)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by notifying the SBM.
- Following the correct procedures by notifying the SBM if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents 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
- 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/carers

Parents/carers are expected to:

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

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

- What are the issues? – [UK Safer Internet Centre](#)
- Online safety topics for parents/carers – [Childnet](#)
- Parent resource sheet – [Childnet](#)

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 and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum within computing sessions and PSHE. (Appendix A)

All schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

In **Key Stage (KS) 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 (KS) 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
- Be discerning in evaluating digital content

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 benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

The safe use of social media and the internet 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. 5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. Regular updates will also be shared via the weekly newsletter.

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

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

6. 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. (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.

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. The PSHE curriculum based on the SCARF program requires teachers to discuss cyber-bullying with their class. (see appendix A)

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying, including 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 (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so 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 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 Electronic devices

Pupils hand their mobile phone to the office each day, staff are not permitted to use mobile phones during lesson times.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Wootton Primary recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We will treat any use of AI to bully pupils very seriously, in line with our anti-bullying and behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

7. 7. Acceptable use of the internet in school

Parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

8. 8. Pupils using mobile devices in school

Pupils in Years 4, 5 and 6 may bring mobile devices into school, but are not permitted to use them during the school day. All mobile phones must be handed in to the class teacher at the start of the school day and these will then be stored in the school office and returned to pupils at the end of the school day.

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. 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:

- Ensuring their device is encrypted – this means if the device is lost or stolen, 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
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates
- External devices such as external hard drives or memory sticks must not be used with school devices.

Staff members must not use the device in any way that 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 SBM.

10. 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 within our 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 code of conduct and 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11.11. Training

11.1 Staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and DDSLs 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.

11.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12.12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the SBM to check if any updates or changes required. It will be formally reviewed by the Governing Body every 3 years.

13.13. 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 A: Online Safety– curriculum coverage

Year Group	Subject Area and Learning Outcomes	DFE Relationships Education and Health Education statutory Requirements
Year R	<u>Keeping safe online</u> • Share ideas about activities that are safe to do on electronic devices; • What to do and who to talk to if they feel safe online.	• The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them. • About the concept of privacy and the implications of it for both children and adults; including that it is not always right to keep secrets if they relate to being safe. • How to recognise and report feelings of being unsafe or feeling bad about any adult. • How to ask for advice or help for themselves or others, and to keep trying until they are heard.
Year 1	<u>Sharing Pictures</u>	• The importance of permission seeking and giving in relationships with friends, peers and adults; • That people sometimes behave differently online, including 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 they 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 and others (including in a digital context); • About the concept of privacy and the implications of it for both children and adults; including that it is not always right to keep secrets if they relate to being safe; • How to ask for advice or help for themselves or others, and to keep trying until they are heard; • That for most people the internet is an integral part of life and has many benefits; • How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private; • That the internet can also be a negative place where online abuse, trilling, bullying and harassment can take place, which can have a negative impact on mental health; • Where and how to report concerns and get support with issues online.
Year 2	<u>Playing games</u>	• 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). • About the concept of privacy and the implications of it for both children and adults; including that it is not always right to keep secrets if they relate to being safe. • How to ask for advice or help for themselves or others, and to keep trying until they are heard. • That for most people the internet is an integral part of life and has many benefits.

		• About the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing. • How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private. • That the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health. • Where and how to report concerns and get support with issues online.
Year 3	<u>Super Searcher</u> • Evaluate the validity of statements relating to online safety; • Recognise potential risks associated with browsing online; • Give examples of strategies for safe browsing online. <u>None of your business!</u> • Know that our body can often give us a sign if something doesn't feel right; to trust these signs and talk to a trusted adult if this happens; • Recognise and describe appropriate behaviour online as well as offline; • Identify what constitutes personal information and when it is not appropriate or safe to share this; • Understand and explain how to get help in a situation where requests for images or information of themselves or others occurs.	• 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. • That for most people the internet is an integral part of life and has many benefits. • How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private. • How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted. • The importance of permission-seeking and giving in relationships with friends, peers and adults. • 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. • 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. • How to recognise and report feelings of being unsafe or feeling bad about any adult. • That the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health. • Where and how to report concerns and get support with issues online.
Year 4	<u>Picture wise</u> • Identify images that are unsafe/safe to share online; • Know and explain strategies for safe online sharing; • Understand and explain the implications of sharing images online without consent.	• The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them. • How information and data is shared and used online. • How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
Year 5	<u>Spot Bullying</u> • Demonstrate strategies to deal with both face-to-face and online bullying;	• The importance of respecting others, even when they are very different from them (for example, physically, in character, personality or backgrounds), or make different choices or have different preferences or beliefs • That people sometimes behave differently online, including by pretending to be someone they are not.

	• Demonstrate strategies and skills for supporting others who are bullied; • Recognise and describe the difference between online and face-to-face bullying. <u>Communication</u> • Understand that online communication can be misinterpreted; • Accept that responsible and respectful behaviour is necessary when interacting with others online as well as face-to-face. <u>Play, Like, Share</u> • Consider what information is safe/unsafe to share offline and online, and reflect on the consequences of not keeping personal information private; • Recognise that people aren't always who they appear to be online and explain risks of being friends online with a person they have not met face-to-face; • Know how to protect personal information online; • Recognise disrespectful behaviour online and know how to respond to it. <u>Is it true?</u> • Understand that the information we see online, either text or images, is not always true or accurate; • Recognise that some people post things online about themselves that aren't true, sometimes this is so people will like them; • Understand and explain the difference between sex, gender identity, gender expression and sexual orientation.	• 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 information and data is shared and used online. • That bullying (including cyberbullying) has a negative and often lasting impact on mental wellbeing. • Why social media, some computer games and online gaming, for example, are age restricted.
Year 6	<u>Facebook friends</u> • Know the legal age (and reason behind these) for having a social media account; • Understand why people don't tell the truth and often post only the good bits about themselves online; • Recognise that people's lives are much more balanced in real life, with positives and negatives. <u>Pressure Online</u> • Understand the risks of sharing images online and how these	• The importance of permission-seeking and giving in relationships with friends, peers and adults. • That people sometimes behave differently online, including by pretending to be someone they are not. • That mental wellbeing is a normal part of daily life, in the same way as physical health. • Why social media, some computer games and online gaming, for example, are age restricted. • How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted. • That people sometimes behave differently online, including by pretending to be someone they are not. • The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.

	are hard to control, once shared; • Understand that people can feel pressured to behave in a certain way because of the influence of the peer group; • Understand the norms of risk-taking behaviour and that these are usually lower than people believe them to be. <u>To Share or not to share?</u> • Know that it is illegal to create and share sexual images of children under 18 years old; • Explore the risks of sharing photos and films of themselves with other people directly or online; • Know how to keep their information private online. <u>Traffic Lights</u> • Identify strategies for keeping personal information safe online; • Describe safe behaviours when using communication technology. <u>Think before you click!</u> • Accept that responsible and respectful behaviour is necessary when interacting with others online and face-to-face; • Understand and describe the ease with which something posted online can spread. <u>It's a puzzle</u> • Identify strategies for keeping personal information safe online; • Describe safe and respectful behaviours when using communication technology.	• 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). • That each person's body belongs to them, and the differences between appropriate and inappropriate or unsafe physical, and other, contact. • How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know. • How to recognise and report feelings of being unsafe or feeling bad about any adult. • 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). • About the concept of privacy and the implications of it for both children and adults; including that it is not always right to keep secrets if they relate to being safe. • How to report concerns or abuse, and the vocabulary and confidence needed to do so. • How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private. • That the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health. • Where and how to report concerns and get support with issues online. • How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private. • 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. • That the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health. • That for most people the internet is an integral part of life and has many benefits
--	---	--

Appendix B: Pupil Device User Agreement Form

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in 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
- 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
- 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

If I bring a personal mobile phone or other personal electronic 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

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

I will immediately let a teacher or other member of staff 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):

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.

Signed (parent/carer):

Date:

Appendix C: Staff Acceptable Use Agreement

Staff Acceptable Use Agreement

- I understand that I must not use the ICT system to access inappropriate content.
- I understand that school information systems and hardware may not be used for private purposes without specific permission from the Headteacher.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. It must not be kept on removable storage devices or attached to emails.
- I will respect copyright and intellectual property rights.
- I understand use for personal finance gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidents of concern regarding children's safety to the DSL.
- I will not communicate with pupils through Instant Messaging, Social Networking, Emails, Texting etc.
- I will promote E-Safety with pupils in my care and will help them to develop a responsible attitude both in and out of School.
- I will store Mobile Devices such as mobile phones securely when not in use.
- I will ensure my Apple/Smart watch is not on during school hours so I cannot receive notification to it
- I will only use school equipment to take pictures of pupils/school events etc.
- I will not use mobile phones in the presence of pupils.
- I will not post negative or unacceptable comments about the school on Social Networking Sites etc.
- I will not contact parents or pupils through Social Networking Sites etc.

I have read, understood and accept the Staff Acceptable Use Agreement

Signed:..... Name:.....
Date:.....