Policy for:

Online Safety

		Date
Reviewed by:	SLT	Autumn 2025
Authorised by:	H&S	Autumn 2025
Date for next review: (or earlier should legislation require it)	Autumn 2026	

Woodstock CE Primary

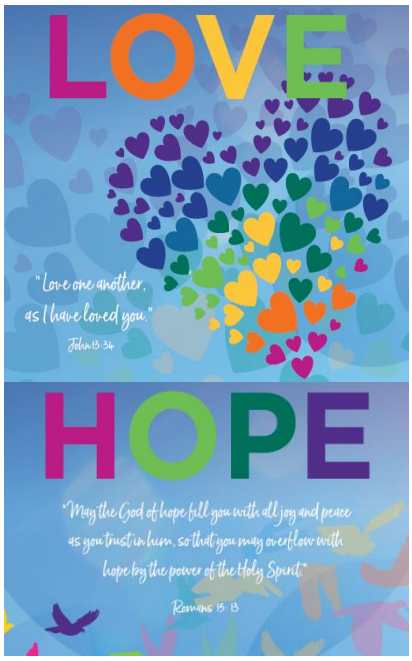
Hand in hand we…
Love | Learn | Flourish

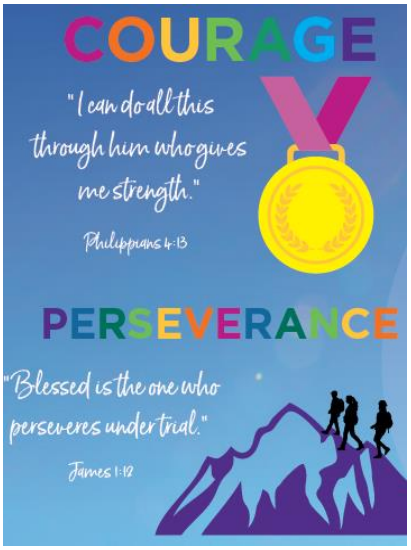
Our Christian Vision & Values

Our Christian vision states that we:
Clear a path for a lifelong journey of exploration and growth, through an innovative and challenging curriculum, inspiring all in our community to be courageous advocates and global citizens. Everyone can find their light and shine it brightly. Hand in hand, we love, learn and flourish together.

'In the same way, let your light shine before others, so that they may see your good works and give glory to your Father who is in heaven.' 'Let your light shine' Matthew 5:16

Our core Christian values allow us to deliver the Christian vision:





Online Safety Policy

Our Vision

We are living in an increasingly connected world where, alongside the benefits of access to technology, come increased risks to children. Lack of guidance and learning in Online Safety can mean children are unaware of the unintended consequences of their on-line behaviour or actions. It highlights the need to educate pupils and the school community about the benefits and risks of using Internet technologies and electronic communications, and provide safeguards and awareness for users, to enable them to control their online experience and their digital footprint.

> ***'Our vision is to make the children at Woodstock School as safe and productive in the on-line world, both in school and outside of school, as they are in the real world with particular focus on protection against grooming, cyberbullying and becoming a positive e-citizen.'***

Our policy and practice against this are clearly articulated in this Online Safety Policy.

Our Aims

Our school ensures that we:

- 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' or other 'mobile devices')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Online Safety

While cybersecurity protects devices and networks from harm by third parties, Online Safety protects the people using them from harm by the devices and networks (and therefore third parties) through awareness, education, information, and technology. It is what we call the appropriate approach to personal safety when using digital technologies.

Online Safety is being aware of the nature of the possible threats that you could encounter whilst engaging in activity through the Internet, these could be security threats, protecting and managing your personal data, online reputation management, and avoiding harmful or illegal content.

It isn't about scaremongering, it isn't about criticism and chaos, it isn't about denying all access; it's about focusing on the positive and enriching side of digital life whilst recognising its challenges and how to best approach them.

Managing Online Risk

The number of people being connected to the internet grows daily (approximately 1,000,000 people per day) as does the need to recognise the challenges facing children – and indeed all of us – in the online space. By practicing Online Safety, we can prevent and mitigate the risks that are inherently involved with using digital technologies, platforms and services. Once the risks are managed, the internet can be enjoyed free from harm and to enormous benefit.

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, anti-Semitism, radicalisation and extremism
- **Contact**: being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. 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 scam

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 (RSE) and health 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 considers the National Curriculum Computing Programmes of Study, our school's curriculum for PSHE & RSE and additional national guidance from online safety organisations such as National Online Safety, NSPCC and CEOP.

Roles and Responsibilities

The Governing Body

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

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

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that 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 the school's safeguarding needs

The governor who oversees online safety is Lynne Hammond.

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, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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

The Headteacher

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

The Designated Safeguarding Lead

Details of the school's DSL and DDSLs are set out in our Child Protection and Safeguarding Policy.

The DDSL 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 Technical Lead (123ICT) 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 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or Governing Body

This list is not intended to be exhaustive.

The ICT Technical Lead (123ICT)

The ICT Technical Lead 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 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

This list is not intended to be exhaustive. The SLT (with support from governors) are responsible for ensuring our 123ICT support is carrying out the expected roles and responsibilities.

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
- Working with the DDSL 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.

Parents

Parents 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
- Act responsibly, in-line with the policy, to ensure any incidents or potential risks, even if taking place outside of school, are made known such that prompt and appropriate action can be taken

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

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).

Educating Pupils about Online Safety

Pupils will be taught about online safety as part of our school's curriculum for computing, PSHE & RSE. The Curriculum information 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

Outline of the Curriculum:

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 age limits for games, apps and how to use basis settings to protect themselves when using devices
- Restrictions of using devices in school and why they are in place (e.g. use of mobile phones)

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.

Educating Parents about Online Safety

As a school we take raising awareness and the profile of Online Safety for parents very seriously, therefore Online Safety guidance and tips are published weekly in our Woodstock Newsletter, Online Safety guidance is available on our school website, and we also engage with outside agencies to provide parent workshops. This policy is shared with parents and available on the school website. 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 DDSL. Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy.)

Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we ensure that pupils understand what it is and what to do if they become aware of it happening to them or others through our school curriculum offer. We 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 actively discusses cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers discuss cyber-bullying at an age-appropriate level with children in-line with our school's curriculum. 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 Online Safety, including aspects of 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 DDSL 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.

Examining Electronic Devices

The Headteacher and SLT, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting (as outline in our Behaviour Policy):

- 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, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from a member of SLT
- 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

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 staff member in conjunction with a member of SLT 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, 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 (or equivalent) immediately, who will decide what to do next. The DSL 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
- Our Behaviour Policy (Section: Confiscation, Searching & Screening)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative 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.

Woodstock CE Primary School 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.

Woodstock CE Primary School will treat any use of AI to bully pupils very seriously, in line with our behaviour policy.

Staff should be aware of the risks of using AI tools while 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 them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our AI usage policy.

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. 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. The ICT Technical Lead (123ICT) 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 school's acceptable use agreements.

Pupils Using Mobile Devices in School

Pupils are not allowed to bring mobile devices into school, however, if for exceptional circumstances, and in agreement with parents, a child requires a mobile device for the journey to and from school, this must be signed in, and out at the school office where it will be kept safely throughout the school day. We do, however, discourage this as much as possible.

Any breach of our schools' rules on this or 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.

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)
- Ensuring their hard drive 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 – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, including those outlined in the Staff Code of Conduct and school's GDPR Policy. 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 ICT Technical Lead (123ICT).

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 the school's Internet Acceptable Use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Any incidents that relate to Child Protection and Safeguarding of Children will be recorded on the school's online system My Concern and will immediately be brought to the attention of the school's DSL/DDSL. Appropriate action will be taken to address and follow up – including sharing of information if appropriate with agencies such as TVP and MASH.

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 (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.

Training

All new staff members will receive training, as part of their induction, on safe online use and online safeguarding issues including cyber-bullying and the risks of online radicalisation this forms part of annual Safeguarding and Prevent training as well as planned-in staff training throughout the year.

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

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

- 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 the risks up
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The Headteacher and 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 – this also includes all volunteers. More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

We have been awarded the 360 Safe Online Accreditation which demonstrates our commitment to keeping our whole school community safe online. The engagement with this process ensures practices are best in class and staff remain at the forefront of latest developments, issues and resources.

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety using our online system My Concern. An incident report log can be found in appendices

This policy will be reviewed every year by the Online Safety Lead (DDSL). At every review, the policy will be shared with the governing body (including the Online Safety Committee). The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links with Other Policies

This Online Safety Policy is linked to our:

- Behaviour Policy
- Anti-bullying Policy
- KCSIE & Child Protection & Safeguarding Policy
- Equality Policy
- Data Protection Policy (GDPR)
- PSHE & RSE Policy
- Acceptable User Policy
- Staff Code of Conduct
- Complaints Policy
- AI usage Policy

Woodstock CE Primary School Online Safety Charter

Safe

- ☆ I will only use the Internet when supervised by a teacher or adult.
- ☆ I will never tell anyone I meet on the Internet my home address, telephone number or my school's name.
- ☆ I will never give my password to anyone, even my best friend, and I will log-off when I have finished using the computer.
- ☆ I will never send anyone my picture without permission from my teacher/parent.
- ☆ I will always be myself and will not pretend to be anyone or anything I am not.
- ☆ I understand that I can only access sites and materials relevant to my work in school and that I will not be able to use the Internet if I deliberately look at unsuitable material or hack into the school's systems.
- ☆ I know that my teacher and the Internet provider will check the sites I have visited.

Meet

- ☆ I will never arrange to meet anyone in person.
- ☆ I understand that the people I communicate with online may not be who they say they are.

Accepting

- ☆ I may not download software from the Internet (including screen savers, games, *.exe files etc.).
- ☆ I may only download video clips and audio clips with the permission of a teacher and only then from a directed website and for educational purposes only.

Reliable

- ☆ I know I cannot trust everything that I see or read on the Internet.
- ☆ I know that information on the Internet may not always be reliable, and sources may need checking.
- ☆ I have the responsibility to provide information that is not misleading, to keep my own data safe and not to misuse any information I have about others.
- ☆ I have the responsibility to check any information before using it.
- ☆ I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.

Tell

- ☆ I will never respond to unpleasant, suggestive, or bullying e-mails and I will always report it to a teacher/parent.
- ☆ If someone says or writes something, not just on the computer but also through texts, which makes me feel uncomfortable or worries I will always report it to a teacher/parent.
- ☆ I will not look for bad language or distasteful images while I'm online and I will report these to a teacher/parent if I come across them accidentally.

I promise to always be **SMART** when using the internet.

SHARED WITH CHILDREN BY THE CLASS TEACHER

PLEASE SIGN YOUR AGREEMENT BELOW

CLASS:_____

Appendices: Staff and Pupil Online Safety Checklist

The following points are discussed with pupils at the start of the school year (and revisited throughout), the start of a project requiring Internet use, or if revision of Acceptable Internet Use is necessary.

- ✓ Only use the Internet when there is a teacher or other adult present to supervise or when you have been given specific permission.
- ✓ Only use your own login name and password. Never use another person's details.
- ✓ Never give out your address, phone number or arrange to meet someone over the Internet.
- ✓ All e-mails, messages in forums and text messages should be polite, appropriate and sensible. Do not send any e-mail or text message which could cause upset.
- ✓ If you receive a rude or offensive message you must report it to a teacher immediately. Do not pass on rude or offensive messages. What may seem funny to you may not be funny to someone else.
- ✓ If you see anything offensive or if you feel uncomfortable about anything, report it to your teacher or to an appropriate member of staff.
- ✓ Be aware that the school may check your computer files and monitor the Internet sites you visit.
- ✓ Ask an adult if you are unsure that a web source is reliable and information you are going to use is accurate.
- ✓ You and your parents should have signed the school Internet Agreement. You will be breaking that Agreement if you deliberately break these rules. This could result in you losing your Internet access at school.

Pupil's attention is drawn to the SMART Class Online Safety which is displayed in every classroom. It is a continuous reminder of our very high-expecations in order to safeguard our children and each other.

Appendices: Online Safety Training Audit of 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?	

Appendices: Reporting Online Safety Incidents

Please record sufficient detail to enable the monitoring of incidents.

Type of Incident:	✓	**System Location:**	✓
Bullying (cyber bullying)		Library	
Grooming		Classroom	
Sharing inappropriate messages		Corridor	
Sending inappropriate images		Outside school premises	
Hacking or virus spreading		Other (record in **description** below)	
Accessing racist, sexual or homophobic material			
Sharing racist, sexual or homophobic material		**Device accessed on:**	✓
Accessing religious hate material		Laptop	
Sharing religious hate material		Desktop computer	
Accessing pornographic material		iPad/Tablet	
Sharing pornographic material		Mobile phone	
Other (record in **description** below)		Other (record in **description** below)	

Date:	**Time:**
Description of what happened:	
Accidental Access:	**Deliberate Access:**

Child/ren Involved:	Year	SEN	Disability	Ethnic Group	Involvement in Incident

Member of staff recording the incident:
Role:

Other staff involved:

Role:

Signed:

Name:

Date:

Status:	✓
Resolved	
Unresolved	
Further intervention needed	
123 ICT informed (if appropriate)	

File THREE Copies (tick when actioned)	**Headteacher**	**Child's File**	**E-safety File**

Details of any subsequent actions or follow-up:
(Include dates)

Action Taken:

If appropriate:	Yes ✓	No ✓
Have you copied Incident Form for class teacher?		
Have you had contact with the parents/carers of all children involved? If Yes, by phone / letter? Date of contact:		
Are any other agencies involved? If Yes, which agencies? If Yes, and the incident was prejudice-motivated, consult Local Authority as to whether a Hate Crime report is appropriate.		
Does the incident require Police/CEOP involvement?		