Policy: Online Safety

Created by:	Kirsten Gibbs (OSL) and Anna Payne (DSL)
Approved By:	Sylvia Greinig (Principal/Proprietor), Fleur Greinig (Head Teacher)
Date Reviewed:	September 2025
Next Review:	September 2026
Review Frequency:	Annually

Contents

Policy: Online Safety....1
Contents....1
Mission Statement....1
Our Core Values....1
Rationale....2
Aims....2
Legislation and guidance....2
Roles and responsibilities....3
Educating children about Online Safety....5
Educating parents/carers about Online Safety....6
Cyber Bullying....6
Acceptable use of the internet in school....7
Pupils using mobile phones in school....7
Staff using work devices outside school....7
How the school will respond to misuse....8
Training....8
Monitoring....9
13. Links with other policies....9
Appendix....9

Mission Statement

At Abbey School our aim is to teach to inspire, motivate and nurture the next generation of creative and critical thinkers. We work in partnership with families/carers and the community to achieve the highest standards. Our main goal is to encourage our children to be resilient, respectful, responsible independent learners, equipped for lifelong learning. Through stimulating, safe learning environments and excellent opportunities to succeed in and out of the classroom, we encourage children's progress and achievements.

Our Core Values

RESPECT, RESPONSIBILITY, RESILIENCE

These 3 core values underpin the ethos of Abbey School. Our young pupils are encouraged to understand these values and how they develop, initially, at the micro level around themselves, their friendships, their families and our school. Later, our older pupils begin to understand how these self-same values affect our

lives on the macro level, with all this means for their lives as they grow into adults and their environment of Devon, the United Kingdom, and also the planet in which we live.

Rationale

The purpose of this policy is to ensure that all staff, parents and children understand and agree the school's approach to e-safety and understand that the policy statement applies to us all, shaping a positive online culture at Abbey School. We believe that young people should never experience abuse of any kind. We recognise that the online world provides everyone with many opportunities; however it can also present risks and challenges. We work in partnership with children, young people, their families, carers and other agencies to promote children's welfare and support them to be responsible in their approach to online safety and develop safe, long-term behaviours.

Aims

Our school aims to:

- Have robust procedures and policies in place to ensure the online safety of pupils, staff and volunteers
- 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.
- Keep abreast of emerging national and local trends and potential risks with regard to online safety and act to support and inform pupils and families 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 (including misinformation and disinformation), racism, toxic masculinity, 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

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.

Roles and responsibilities

The Principal/Proprietor

The Principal/Proprietor has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. They will ensure a whole school approach to online safety; making sure that online safety (and training) is integrated, aligned and considered as part of the whole school safeguarding approach and relevant policies and procedures.

The Principal/Proprietor 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. Inductions and training are in line with advice from Torbay Safeguarding Children Partnership.

The Principal/Proprietor 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 Principal/ Proprietor has regards to the Teacher's Standards, setting out the expectation that all teachers manage behaviour effectively to ensure a good and safe educational environment with a clear understanding of the needs of all pupils.

The Principal/Proprietor 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 Principal/Proprietor should ensure children are taught how to keep themselves and others safe, including keeping safe online, recognising that this must be tailored to the specific needs and vulnerabilities of individual children: e.g. those who are victims of abuse, those with SEND, those who are looked after children.

The Principal/Proprietor 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 Principal/Proprietor will review the DfE filtering and monitoring standards, and discuss with OSL/ DSL and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually; additional reviews will be made following the introduction of new devices or safeguarding reports
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Principal/Proprietor should ensure that the filtering and monitoring systems in place do not "over block": leading to unreasonable restrictions about what children can be taught.

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 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 OSL, headteacher and Principal/ Proprietor 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
- Working with the headteacher, outsourced ICT management 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
- Ensuring that any online safety incidents are logged (see appendix 1) 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 2 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 headteacher
- 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.

Outsourced ICT Management

The Outsourced ICT Management Companies (Think IT and BT) are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which 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
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

The Online Safety Lead (OSL)

The Online Safety Lead is responsible for:

- Ensuring that any online safety incidents are logged (see appendix 1) 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
- Performing filtering tests are performed monthly on a variety of different devices around the school (appendix 8)
- Working with the DSL, headteacher and Principal/ Proprietor to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Working with the Outsourced ICT management to make sure the appropriate systems and processes are in place
- Managing all online safety issues and incidents in line with the school's child protection policy
- Undertaking annual risk assessments that consider and reflect the risks children face
- Distributing surveys to gain feedback from parents and pupils on an annual basis.
- Providing Head Teacher with relevant online safety information that should be shared with Parents/Carers

- Perform weekly monitoring checks of the history of a random selection of devices (appendix 7)
- Perform weekly key word checks to ensure the effectiveness of the filtering system (appendix 6)

This list is not intended to be exhaustive.

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 4 and 5)
- 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 reporting this verbally to the DSL (safeguardingteam@abbeyschool.co.uk) and/or OSL (kirstengibbs@abbeyschool.co.uk)
- Following the correct procedures by contacting the OSL 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 (see appendix 1) 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/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 (appendices 4 and 5)

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
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Families can find specific information about online safety on our website. Helpful updates are also shared on Abbey School's social media accounts. The Headteacher is the only member of staff with access and monitors both the Facebook and Instagram accounts. The children are never identified by name. There are filters in place that prevents negative comments, inappropriate words and spam from being posted.

Parents/carers are encouraged to utilise the National Online Safety website (National Online Safety | Keeping Children Safe Online in Education) to further their own knowledge and confidence.

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 children about Online Safety

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

All schools have to teach:

- Relationships education and health education in primary 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 2 (KS2)** 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, and also of risks associated with artificial intelligence (AI) – further outlined in our AI policy.
- How information and data is shared and used online (including misinformation and disinformation).
- 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 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 or who are looked after children.

Abbey School takes advantage of Safety Internet Day to reinforce what the pupils have already explored in their time at school.

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 and Facebook site. This policy will also be shared with parents/carers.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- 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

If parents/carers 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.

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 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. Class teachers will discuss cyber-bullying with their tutor groups.

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 (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.

Acceptable use of the internet in school

At this time, Abbey School do not utilise remote learning. However, apps such as 'Seesaw' and 'Google Classroom' are used within the curriculum, and to keep a record of children's learning. All 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 (appendices 3 to 5). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Each year group creates their own relevant set of rules for using ICT systems appropriately in class and pupils sign their agreement here. All pupils are additionally encouraged to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 4 and 5) to allow them to increase their responsibility in this area.

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.

More information is set out in the acceptable use agreements in appendices 3 to 5.

Pupils using mobile phones in school

Pupils are not permitted to have mobile phones in school, unless prearranged between Parents/Carers and school, and they must be locked away in the office during the school day.

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 by always installing the latest updates

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 Headteacher.

How the school will respond to 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 ICT acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. All incidents will be recorded in the Log of Internet History (appendix 7).

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. 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.

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, newsletters 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 deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

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

Staff are required to undertake an online safety training course online. DSL and deputies, OSL, SENCO and Headteacher will undertake a more in-depth training provided on the National Online Safety website (National Online Safety | Keeping Children Safe Online in Education) and all remaining staff on 'The Key' website.

Monitoring

The DSL and OSL log behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 1.

This policy will be reviewed every year by the Principal / Proprietor. 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.

At Abbey School we utilise Physical Monitoring to ensure that pupils are safe in education, as such pupils do not use technology unsupervised in school. We ensure that recognised vulnerable pupils are additionally kept safe by 1:1 monitoring when working online.

A whole school approach towards monitoring and managing effective filtering is maintained.

Should the use of the internet result in a pupil viewing content that is deemed inappropriate, pupils are encouraged to share these occasions with an adult and we, as a school use these incidents to support the pupils for future and thus is viewed as a learning opportunity for the pupil/pupils. All incidents are recorded in The Log of Internet History (appendix 7).

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
- Personal, Social, Health and Economics Education (PSHE)
- Artificial Intelligence (AI) policy
- Child-friendly E-Safety Policy
- Child-friendly Safeguarding Policy

Appendix

1. Online Safety Incident and Concern Log

2. Staff audit

3. Acceptable Use Agreements for Staff/ Volunteers/ Visitors

4. Acceptable Use Agreements for EYFS / KS1 Pupils

5. Acceptable Use Agreements for KS2 Pupils

6. Key Word Check Form

7. Online Safety Log of Internet History

8. Log of Internet Filtering

Online Safety Incident and Concern Log

Date	Log	Risk Assessment	Actions Taken/Decisions Made	Reviewed Risk	Persons

Online Safety Training Needs Audit

Name of staff member:	**Date**:	
Question	**Yes/No/**	**Comments**
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/carers?		
Are you familiar with the filtering and monitoring systems on the school's devices and networks?		
Do you understand your role and responsibilities in relation to filtering and monitoring?		
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?		

Completed online: https://forms.gle/bT7Wj9ZfBwjFtnpP8

Staff Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF	
Name of staff member:	
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 online safety lead know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member):	**Date:**

Reception Class & Infants Acceptable Use Agreement

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

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• 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
• Never download an app, picture or video without asking an adult.
• I will only take a photograph or video of someone if they say it is okay.
• 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.	

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 will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Juniors Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell an adult immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it • Ask other people for permission to take their photo or a video and respect their wishes. • Always treat the school's ICT equipment (such as iPads) with respect and tell an adult if something doesn't work or is broken. **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Download any apps, images or videos without the permission of an adult • Open any attachments in emails, or follow any links in emails, without checking with an adult. • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is harmful, offensive or otherwise inappropriate • Log in to any learning apps using someone else's details **If I bring a personal mobile phone or other personal electronic device into school:** • I understand it will be kept in the school office until home time. • I will not wear a smart watch or fit bit. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Key Word Check

Date:	Person (s) checking:	Details of checks undertaken:	Risk to internet users: No risk Low risk Medium risk High risk	Actions following checks:	Reviewed risk following actions: No risk Low risk Medium risk High risk

Log of Internet History Monitoring

Date:	Person (s) checking:	Details of checks undertaken:	Risk to internet users: No risk Low risk Medium risk High risk	Actions following checks:	Reviewed risk following actions: No risk Low risk Medium risk High risk

Log of Internet Filtering

Date:	Person (s) checking:	Details of checks undertaken:	Risk to internet users: No risk Low risk Medium risk High risk	Actions following checks:	Reviewed risk following actions: No risk Low risk Medium risk High risk