THORPE HALL SCHOOL

Online Safety Policy

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Ensure the safe, ethical and responsible use of artificial intelligence (AI), recognising both its educational benefits and safeguarding risks
- Develop pupils' critical awareness of AI generated- content, including misinformation, bias and fabricated media

The 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
- Exposure to **AI generated harmful, misleading- or fabricated content**, including deepfakes and synthetic media
- Biased, inaccurate or hallucinated AI outputs presented as fact

This now includes misinformation, disinformation, and conspiracy theories, which can distort children's understanding and influence harmful behaviours.

- **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
- Interaction with **AI chatbots or avatars** that simulate human behaviour in unsafe or manipulative ways
- **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;
- Use of AI to impersonate others, generate abusive material, create hoaxes or support cyberbullying
- Academic dishonesty through unauthorised AI use
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam
- AI enabled scams, phishing and impersonation fraud

Legislation and Guidance

This policy is based on the Department for Education's (DfE) 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
-
- DfE guidance on **Generative Artificial Intelligence in Education**

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 students' electronic devices where they believe there is a 'good reason' to do so.

Roles and Responsibilities

The Board of Governors

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

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

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

The governing board 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 filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

The school will use the DfE's 'Plan Technology for Your School' tool to assess and improve filtering and monitoring systems. All changes to filtering settings will be logged and reviewed by the Online Safety Group.

- 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.
- Ensures **AI related online safety risks** are included in filtering, monitoring and safeguarding reviews

The governor who oversees online safety is Mr Hampshire-Waugh.

All governors will:

- Ensure they have read and understand this policy
- 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
- 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 students 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 Leads

Details of the School's DSL and Deputies are set out in our Child Protection and Safeguarding Policy as well as in relevant job descriptions.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher and Governing Board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Managing all online safety issues and incidents in line with the school child protection policy
- 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

- 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
- Takes lead responsibility for **AI related- safeguarding concerns**, including deepfakes and AI enabled- bullying
- Ensures AI elated- incidents are logged and escalated appropriately
- Providing regular reports on online safety in school to the Headteacher and/or Governing Board

This list is not intended to be exhaustive.

The Online Safety Lead (OSL) will:

- lead the Online Safety Group
- work with the Designated Safeguarding Leads (DSLs), receive reports of online safety issues to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to SLT and the Governing Body.

- The Online Safety Group has the following members:
- Designated Safeguarding Lead Senior and Prep
- Online Safety Lead
- Online Safety Governor
- Technical staff
- Learners (When invited)

Members of the Online Safety Group will assist the DSL/OSL with:

- the production/review/monitoring of the school Online Safety Policy/documents

- the production/review/monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

The ICT/Systems Manager

The ICT Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students 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

The ICT Manager will ensure compliance with the DfE Cyber Security Standards, including annual penetration testing and staff training on phishing awareness.

- 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
- 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
- Blocks or restricts **unapproved or unsafe AI tools** and monitors AI platform use

This list is not intended to be exhaustive.

All Staff and Volunteers

All staff, (including agency staff, and volunteers- synopsis in training) 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). All staff and volunteers will ensure that students follow the school's terms on acceptable use (appendices 1 and 2).
    - Working with the DSL to ensure that any online safety incidents are logged (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
- 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'
- Verify accuracy and appropriateness of any AI generated- content
- Never rely on AI for safeguarding, behaviour or assessment decisions

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 (appendices 1 and 2)

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
- Healthy relationships – Disrespect Nobody

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).

Artificial Intelligence (AI)

Generative AI tools (e.g. chatbots, image and video generators) are increasingly accessible. While AI can enhance learning and efficiency, it also presents online safety and safeguarding risks.

The school recognises the following risks:

- Deepfake creation and distribution
- Harmful, sexualised, extremist or abusive AI generated content
- Misinformation or fabricated outputs
- Data protection breaches where personal data is entered into AI tools

AI misuse causing harm, distress, deception or safeguarding concern will be managed in line with the **Behaviour Policy, Antibullying Policy and Safeguarding Policy**.

Educating Pupils About Online Safety

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

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
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- Understand that AI outputs may be **inaccurate, biased or fabricated**
- Recognise and report **AI generated abuse or deepfakes**
- Use AI tools ethically, transparently and with adult permission
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- Understand that AI outputs may be **inaccurate, biased or fabricated**
- Recognise and report AI generated abuse or deepfakes
- Use AI tools ethically, transparently and with adult permission

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of Senior School**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

Educating Parents About Online Safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy is available on our website.

The school will host online safety workshops for parents and keep them regularly updated by-

- Raising awareness of online risks.
- Sharing resources and guidance.
- Use of AI to impersonate others, create fake images/audio/video or amplify abuse
- Encouraging safe practices at home.

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

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 intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power (as outlined in the School's Behaviour Policy).

Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students 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 students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their 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, Relationships and Sexual Education (RSE) 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 so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the School will follow the processes set out in the School Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the School will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the SLT to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.

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

- The DfE's latest guidance on screening, searching and confiscation

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

Artificial Intelligence (AI)

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

Thorpe Hall School recognises that AI has many uses to help students learn but may also have the potential to be used to bully others. For example, Use of AI to impersonate others, create fake images/audio/video or amplify abuse

Thorpe Hall School will treat any use of AI to bully students in line with our Anti-Bullying Policy.

Staff must refer to the DfE's guidance on generative AI and complete a risk assessment before introducing any AI tools into teaching or administration. AI must not be used to process sensitive students' data without explicit consent and oversight.

Acceptable Use of the Internet in School

All students (from Year 5 upwards), staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the School's ICT systems and the internet (appendices 1-3). 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 students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

Students Using Mobile Devices in School

Students may bring mobile devices into school but are not permitted to use them during school time. They should be switched off and out of sight. This includes:

  - Lessons
  - Tutor group time
  - Break/Lunch time
  - Clubs before or after school
- Travel to and from fixtures, or any other activities organised by the school (an exception may be made by a trip leader for senior school students under specific criteria and in line with the acceptable use policy)

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the Acceptable Use agreement by a student 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)
- 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, as set out in appendix 3. The policy can be found in the employment policies section of the staff handbook on https://yourhr.space/thorpehall/

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 ICT manager.

How the School will Respond to Issues of Misuse

Where a student misuses the School's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and Acceptable Use 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

Serious AI misuse (deepfakes, sexual content, data breaches) may be escalated to external agencies or police

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 internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

As part of safer recruitment, the school may conduct online checks on shortlisted candidates. All data gathered will be handled securely and in line with GDPR.

All staff members will receive refresher training biannually 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
- **AI risks, deepfakes, data protection and verification of AI outputs**
- 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 students 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 DSL and their 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.

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.

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to blocked activity for students and staff. An incident report log (appendix 5) is used for any other surrounding online incident.

AI related incidents are monitored as part of safeguarding oversight

This policy will be reviewed every year by the Leadership Team and ICT/Systems Manager. At every review, the policy will be shared with the Governing Board. The review (such as the one available here) 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:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Staff Disciplinary Policy
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- EYFS – Camera, Mobile Phone and photography Policy
- PSHE / RSE Policies
- Curriculum Policy
- **Whole-School Artificial Intelligence (AI) Policy**

Policy Revised:	May 2026
Policy Approved:	May 2027
Next Review Date:	May 2028

Appendix 1: EYFS, KS1 and Lower KS2 acceptable use agreement (pupils)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS
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 click on 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
- 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

Student Pledge for iPad Use:

- I will take good care of the iPad
- I understand that the iPad is subject to inspection at any time without notice.
- I **will not** photograph or video anyone unless in context of a lesson and directed by a teacher.
- I **will never** share any images or movies of people in a public space on the Internet, unless I am asked to do so by my Teacher.

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

Appendix 1(b): Y5 and 6 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS		
Name of pupil:	**Apple ID**	

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 username 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 a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Only use AI tools and platforms or AI features embedded within software when asked by a teacher
- I understand that unauthorised, deceptive or harmful AI use is a breach of acceptable use expectations.
- Always log off or shut down a computer when I'm finished working on it

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
- 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
- Create, link to or post any material that is offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

Use of personal devices:

- Personal mobile devices, whether smart phones, tablets, smart watches or similar are not allowed to be used in school. If you need to make a phone call home for some reason then you should ask the office permission to use the school phone; you will not be charged for this.
- It is important to understand that this policy covers the sending of TEXTS during the school day – this is not allowed. All personally-owned smart phones, mobile or similar devices should either be handed in on arrival or not brought to school at all.
- Mobile devices will not be used or taken on any school trip or visit

Student Pledge for iPad Use:

- I will take good care of the iPad
- I understand that the iPad is subject to inspection at any time without notice.
- I **will not** photograph or video anyone unless in context of a lesson and directed by a teacher.
- I **will never** share any images or movies of people in a public space on the Internet, unless I am asked to do so by my Teacher.

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

Appendix 2: KS3 & KS4 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS		
Name of pupil:	**Apple ID**	**Password**

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 username 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 a teacher (or sensible 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'm finished working on it
- Only use AI tools and platforms or AI features embedded within software when asked by a teacher
- I understand that unauthorised, deceptive or harmful AI use is a breach of acceptable use expectations.

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
- 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
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

Use of personal devices:

- Personal mobile devices, whether smart phones, tablets, smart watches or similar are not allowed to be used in school. If you need to make a phone call home for some reason then you should ask the office permission to use the school phone; you will not be charged for this.
- It is important to understand that this policy covers the sending of TEXTS during the school day – this is not allowed. All personally-owned smartphones, watches or similar devices should be switched off at the gate and not switched on until they have left the premises.
- If permission is given by the group leader, mobile devices may be used on school trips for music and appropriate entertainment under acceptable use agreements
- I **will never** share any images or movies of people in a public space on the Internet, unless I am asked to do so by my Teacher.
- I will abide by the Online safety policy on the school website.

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

Serial Number:	Model	Charger and Case -
Signed (pupil):		**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
▪ I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. ▪ I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. ▪ I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. ▪ I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs 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. ▪ These agreements explicitly apply to: AI tools and platforms and AI features embedded within software ▪ Unauthorised, deceptive or harmful AI use is a breach of acceptable use expectations. ▪ I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

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

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?	
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?	

Appendix 5: online safety incident form

Online FORM

E-Safety Incident Log Form

Name of person reporting incident:	
Names of User(people involved):	
Date and time of incident: Date incident reported:	
Website visited or Searched terms?	
Details of incident, including evidence:	
Location and device details:	
Clarification of the risk or breach e.g. does it relate to safeguarding, bullying, inappropriate content, data protection, copyright, infringement, sexting, etc? (Use 3Cs categorisation):	
Initial action taken and current status:	
Resolution of incident:	

AI Risk Assessment (Linked to Online Safety Policy)

This Risk Assessment supports and is referenced by the Online Safety Policy, ensuring AI-related risks are identified, controlled and reviewed.

Risk Description

Likelihood

Impact

Controls

Owner

Review Date