Stanstead

Flying High Academy

Online Safety Policy

September 2025

To be reviewed September 2026

At Stanstead Flying High Academy, we are committed to ensuring equality of education and opportunity for all pupils, staff, parents and carers receiving services from the school, irrespective of race, gender, disability, faith or religion or socio-economic background. We aim to develop a culture of inclusion and diversity in which all those connected to the school feel proud of their identity and able to participate fully in school life. All aspects of this policy are linked to our safeguarding policies and procedures and adhere to Keeping Children Safe in Education (KCSIE latest version).

Computing (including Online Safety) Vision:

We are committed to providing opportunities that enables all pupils to achieve every day that will not only ensure our children are secondary ready, but also prepare them for life in what will be their modern Britain.

Our goal is for pupils to use technology in an appropriate and safe way to enhance their learning, resulting in a deeper understanding and enabling them to be prepared for the evolving world of technology.

Aims

The aim of this Policy is to ensure everyone understands and is clear about responsibilities when using the internet to support learning, or as part of routine working practices, and the action and strategies taken by the school to safeguard children.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

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 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.

This policy complies with our funding agreement and articles of association.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors:

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, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;

- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Headteacher

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

The headteacher:

- has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the Online Safety Lead.
- as Designated Safeguarding Lead and the Deputy Safeguarding Lead are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- will receive regular monitoring updates from the Online Safety Lead.

The Designated Safeguarding Lead:

Stanstead's Designated Safeguarding Lead is Tanya Smith and the Deputies are Kerry Miller and Will Smee.
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
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Flying High Partnership, IT Services and Development Manager and L.E.A.D IT Services to make sure the appropriate systems and processes are in place
- Working with the headteacher, L.E.A.D IT Services 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 3) 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 board
- 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.

The IT Services and Development Manager

The IT Services and Development Manager is 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
- Ensuring that any online safety incidents are logged and reported to the DSL
- 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.

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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- 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 an urgent issue with the L.E.A.D IT Services helpdesk.
- Following the correct procedures by logging service request with the L.E.A.D IT Services helpdesk if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Pupils:

- are responsible for using the school digital technology systems in accordance with the Student/Pupil Acceptable Use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the School's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers:

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

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

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 2).

Educating Pupils about Online Safety

Our Online Safety policy is a crucial aspect of our computing curriculum and ensures that all of our pupils use technology safely and understand the risks associated with using computers and are educated to avoid and minimise such risks to themselves and others.

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

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

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

- That people sometimes behave differently online, including by pretending to be someone they are not

- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will 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.

Our pupils will use Project Evolve, supported by National Online Safety, where they will learn about online safety through the following modules:

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security
- Copyright and ownership

To supplement this, our pupils will use CEOP's Think U Know, UK Safer Internet Centre and Be Internet Awesome by Google to develop their understanding of online safety.
In addition, we will share weekly guides from National Online Safety that alert and educate parents to current and topical online safety issues.
Furthermore, we will discuss an online safety scenario at the start of each Computing lesson.

Education – parents/carers

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. 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.

Cyberbullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

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 classes.

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 makes available information 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.

Examining Electronic Devices

The headteacher, 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:

- 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:

- Make an assessment of 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 the headteacher.
- 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 co-operation

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 headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, 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/carer 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

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

Technical – infrastructure / equipment, filtering and monitoring

With guidance from Flying High Partnership and L.E.A.D IT Services, the school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that procedures and expectations identified within this policy are implemented. It will also ensure that the relevant people with specific responsibilities, effectively carry out their e-safety responsibilities.

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements. There will be regular reviews and audits of the safety and security of technical systems. Servers, wireless systems and cabling will be securely located and physical access restricted. All users will have clearly defined access rights to school technical systems and devices.

Internet access is filtered for all users. Illegal content (child sexual abuse images and explicit or violent content) is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.

Artificial Intelligence (AI) in Education – Guidance & Acceptable Use

Approved use of AI

While generative AI tools can streamline and expedite various written tasks, they do not substitute for the expertise and discretion of human professionals. Whatever tools or resources are used to produce plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produced it. Any member of staff, trustee or local governor using an AI-generated plan, policy or document should only share the AI-generated content with other members of staff, trustees or local governors for use if they are confident of the accuracy of the information, as the content remains the professional responsibility of the person who produced it.

Permitted Uses of Microsoft Copilot (with a licensed account- connected to a work email address):

- Creating and refining lesson resources
- Summarising meeting notes or CPL readings
- Generating planning templates or policies
- Strategic school/partnership tasks
- Supporting administrative tasks
- Support the analysis of anonymised data.

Other Generative AI Systems (e.g., ChatGPT, Gemini, Claude)

- Use of third-party generative AI tools should be:
- For non-identifiable content only
- Never used to upload or generate content from personal, pupil, or school-sensitive data
- In alignment with DfE guidance, GDPR, data protection and FHP safeguarding procedures

Prohibited Use

- Utilising work produced, without personalising, checking and ensuring accuracy.
- Resources development without human oversight.
- Use AI for formative or summative assessment without human moderation
- Use AI tools with pupils unless content has been pre-reviewed and quality assured.
- Illegal or harmful activities which deviates from our commitment to British Values and prevention of radicalisation.
- Inputting deliberately biased content, which may influence the training of the AI.
- Generate content to impersonate, bully or harass another person
- Generate explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt

Staff Training

All staff must exercise due diligence when integrating AI systems into educational settings, recognising the limitations and possible unintended consequences of these technologies. Clear protocols should be established for the development, review, and deployment of AI driven resources, ensuring that all content meets established standards for accuracy, appropriateness, and alignment with institutional values. Ongoing professional development is essential to maintain staff awareness of emerging risks, evolving best practices, and the ethical landscape surrounding AI in education. The areas covered by the training will equip staff with the knowledge and skills needed to use

AI safely and effectively in educational settings.

Educating pupils on AI

Educating students about artificial intelligence should encompass its capabilities, potential advantages, and inherent risks, with an emphasis on ethical considerations and the promotion of responsible usage. Instruction should include an overview of AI's operational principles, its diverse applications across multiple sectors, and awareness of issues such as bias, privacy concerns, and possible over-dependence. Fostering critical thinking and digital literacy is essential to equip learners to effectively navigate the complexities of AI.

Acceptable Use Policy

All pupils, 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 1 to 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 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 1 and 2.

Mobile technologies

Mobile phones are not permitted to be used in the school setting. Staff are permitted to use their mobile phones in the office and in the staff room area. Lockers and trays are provided by the school for staff to use at the beginning and end of the school day. Taking video or photographs on mobile phones is strictly prohibited anywhere within the school setting. School emails should not be set up on staff's mobile phones unless a login and security passcode is required.

At Stanstead, we would prefer that no child brings a mobile phone to school. However, we recognise that some parents who allow their child to go home alone (in accordance with school policy) are reassured in the knowledge that their child has a mobile phone with them on their journey home. Therefore, in these circumstances only, we allow for selected children to bring a mobile phone to school.

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
- Lock the device before leaving it unattended
- Not sharing the device among family or friends
- Allowing operating systems to be up to date by always rebooting when notified to so by administrator notifications

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 2.

If staff have any concerns over the security of their device, they must seek advice from Flying High Partnership, IT Services and Development Manager. This could include but not limited to ensuring their laptop is encrypted, ensuring laptop locks if left inactive for a period of time, checking antivirus is active.

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 ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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 disciplinary procedures and 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, 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 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.

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 of policy

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 3.

This policy will be reviewed every year by the Headteacher and Online Safety Lead. At every review, the policy will be shared with the governing board. The review will be supported by an annual 3rd party 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 disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Anti-Bullying and Cyber-Bullying policy

This policy is in line with KCSIE 2025.

Review Date: September 2026

Appendix 1: Child and Parent acceptable use agreement

Key Stage 2 Online Safety Agreement 2025– 2026

Both pupils and their parents/carers are asked to sign to show that the online safety rules on the reverse of this agreement have been understood and agreed.

Consent for internet access and related technologies

I have read and understood the school's online safety rules and give permission for my child to access the internet and e-mail and message accounts as part of the school curriculum. I understand that the school:

✓ Will take all reasonable precautions to ensure that pupils cannot access inappropriate materials.

✓ Cannot be held responsible for the content of the materials accessed through the internet.

I agree that the school is not liable for any damages arising from use of the internet facilities.

✓ May use monitoring software to ensure that inappropriate materials are not being stored or used on school equipment.

I understand that if my child fails to follow the Online Safety rules that this may result in them not being permitted to use computers, the Internet and other new technologies in school.

Please print name_____

Signed by Parent/Carer _____ Date_____

Pupil Online Safety Rules 2025– 2026

Think then click

We use computers, the internet and lots of other new technologies to help us

learn. To keep us safe when using them we must:

- Ask permission before using the internet.
- Only use websites that an adult has chosen.
- Tell an adult if we see anything we are uncomfortable with.
- Only e-mail and message people an adult has approved. Only send emails and messages that are polite and friendly.
- Do not open e-mails that are sent by anyone we do not know.
- Never give out personal information or passwords.
- Never arrange to meet anyone we do not know.
- Do not use internet chat rooms or any social networking sites.
- Do not use any inappropriate language when communicating online.
- Always log off or shut down a computer when I've finished working on it.

Pupil's agreement:

- I have read and I understand the Online Safety rules.
- I will use the computer, network, internet access and other new technologies in a responsible way at all times.
- I know that network and internet access can be monitored.
- If I fail to follow these rules, then I may not be allowed to use the computer, network, internet or other new technologies in school.

Pupil name:_____ Class:_____

Signed by pupil_____ Date:_____

Appendix 2- Staff and Governor acceptable use agreement

Acceptable Use Policy – Staff, Governor and ICT Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our working life in school. This policy is designed to ensure all staff are aware of their professional responsibilities when using any form on ICT. All staff and governors are expected to sign this policy and adhere at all times to its contents.

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/ parent permissions 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 will ensure that my online activity both in school and outside will not bring my professional role into dispute.

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.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

• I will report any incidents of concern regarding children's safety to the online safety co-ordinator (Gemma Rolley – Online Safety Leader) or the Headteacher.

• I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.

User Signature:

I agree to follow the code of conduct and support the safe use of ICT throughout the school.

Full Name:_____

Job Title:_____

Signature:_____Date:_____

Appendix 3- Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**