

## SHS B19 - Online Safety Policy

This policy is applicable to all pupils, including those in EYFS.

St Hugh's School works with children and families as part of its activities. These include, but are not limited to:

- Onsite educational activities, including:
  - Classroom teaching
  - Sporting activities
  - Extra-curricular activities, including after school clubs
- Offsite activities, including:
  - Educational field trips
  - Residential trips
  - Sporting fixtures and away activities

### **The purpose of this policy statement is to:**

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, digital devices, online platforms and emerging technologies;
- provide staff and volunteers with the overarching principles that guide our approach to online safety;
- ensure that, as an organisation, we operate in line with our values, safeguarding responsibilities and legal obligations in terms of how we use online devices, systems and services;
- explain how St Hugh's School protects and educates pupils, staff and the wider school community in their use of technology, and how concerns are identified, recorded, managed and escalated.

The policy statement applies to all staff, volunteers, pupils, parents and carers, visitors and anyone involved in St Hugh's School's activities.

### **Legal framework**

This policy has been drawn up based on legislation, statutory guidance, policy and sector best practice that seeks to protect children in England. It should be read in particular alongside:

- Keeping Children Safe in Education;
- Working Together to Safeguard Children;
- The Education Acts and the Independent School Standards Regulations;
- The Prevent Duty and related guidance on protecting children from radicalisation and extremism;

- UK GDPR and the Data Protection Act 2018;
- The Online Safety Act 2023, noting that the Act places duties primarily on regulated online services and platforms, but is relevant context for children's online safety;
- Department for Education digital and technology standards, including filtering and monitoring and cyber security standards;
- UK Safer Internet Centre guidance on appropriate filtering and monitoring.
- [online abuse](#)
- [cyber bullying](#)
- [child protection](#)

### We believe that:

- children and young people should never experience abuse of any kind;
- children should be able to use the internet and digital technology for education and personal development, but safeguards need to be in place to ensure they are kept safe;
- online safety is an integral part of safeguarding and should be embedded within the school's culture, curriculum, staff training, technology arrangements and governance oversight.

### We recognise that:

- the online world provides many opportunities; however, it can also present risks and challenges;
- online safety risks are broad and continue to evolve, including risks linked to content, contact, conduct and commerce;
- children may be exposed to illegal, inappropriate or harmful content, including pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, extreme violence, misinformation, disinformation, conspiracy theories and AI-generated content;
- children may be subjected to harmful online interaction, including grooming, exploitation, peer pressure, bullying, harassment or harmful interaction through online platforms or generative AI applications;
- online behaviour can increase the likelihood of harm, including online bullying, sharing nudes and semi-nudes, non-consensual image sharing, deepfakes and other forms of digitally enabled abuse;
- commerce-related risks include online gambling, inappropriate advertising, phishing, fraud and financial scams;
- we have a responsibility to help keep children and young people safe online;
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online;

- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse;
- children with SEND or additional vulnerabilities may require adapted teaching, supervision, support or reporting routes to help them stay safe online;
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and helping young people to be responsible in their approach to online safety.

**We will seek to keep children and young people safe by:**

### **Filtering and monitoring**

St Hugh's School recognises that appropriate filtering and monitoring are essential parts of online safeguarding. Filtering is preventative and seeks to block access to illegal, inappropriate or harmful online content. Monitoring is reactive and helps the school to identify concerning activity, behaviour or attempted access so that appropriate action can be taken.

- identify and assign roles and responsibilities for managing filtering and monitoring arrangements;
- ensure the governing body/proprietors, senior leaders, the DSL and IT support understand their respective responsibilities for filtering and monitoring;
- review filtering and monitoring provision at least annually and when there is a significant change in technology, risk, provision or pupil need;
- ensure filtering systems block illegal, inappropriate and harmful content without unreasonably restricting teaching, learning or legitimate safeguarding education;
- ensure monitoring strategies are proportionate to the school's safeguarding needs, age range, device use and risk profile;
- check that filtering and monitoring systems work in practice, including on school-owned devices and networks;
- ensure that alerts, reports or concerns arising from filtering and monitoring are reviewed and escalated to the DSL where they indicate a safeguarding concern;
- consider the risks posed by personal devices, mobile data, encrypted applications, app-based activity and bring-your-own-device arrangements;
- ensure that school-owned devices are managed appropriately and kept secure, updated and protected;
- take account of risks linked to AI-generated content, misinformation, disinformation and emerging technologies when reviewing filtering and monitoring provision.
- Filtering and monitoring arrangements will be discussed as part of the school's safeguarding governance and review arrangements.

### Mobile phones, personal devices and school devices

The school recognises that many children have access to the internet through mobile data and smart technology, which may bypass school filtering and monitoring systems.

- set clear expectations for pupil use of mobile phones, smart technology, wearable devices, cameras and other digital recording devices;
- manage boarding pupil mobile phone use in line with the Mobile Phone Acceptable Use Policy for Boarding Pupils;
- expect staff to use school systems and school devices for school business wherever possible;
- expect staff to follow the Staff Code of Conduct and Acceptable Use Policies when using any device in connection with school work;
- prohibit the use of personal devices in contexts where this could compromise safeguarding, privacy, professional boundaries or data protection;
- ensure that any use of school-owned devices by pupils is appropriately supervised, filtered, monitored and supported;
- require concerns about misuse of devices, online peer abuse, harmful content, bullying, harassment or inappropriate image sharing to be reported in accordance with safeguarding procedures.

### Cyber security and information security

Cyber security forms part of the school's safeguarding and operational risk management arrangements. Protecting school systems helps to protect pupils, staff, personal data and the continuity of education.

- maintain appropriate technical and organisational measures to protect school systems, accounts and data;
- expect staff and pupils to use strong passwords and maintain account security;
- require suspected phishing, account compromise, malware, data breaches or cyber incidents to be reported promptly;
- provide staff with appropriate cyber security awareness and updates;
- restrict access to systems and data according to role and need;
- ensure school systems and devices are updated, supported and protected as far as reasonably practicable;
- consider cyber security risks when adopting new platforms, systems, services or AI tools.

### If online abuse or an online safety incident occurs, we will respond to it by:

- following the school's safeguarding procedures, including recording concerns and decisions appropriately;

- ensuring that online and e-safety incidents are passed to the DSL where they raise a safeguarding concern;
- providing support and training for staff and volunteers on dealing with all forms of online abuse, including bullying/cyberbullying, emotional abuse, sharing nudes and semi-nudes, sexual abuse, sexual exploitation, grooming, harassment, deepfakes and AI-generated harmful content;
- making sure our response takes account of the needs and wishes of the child experiencing abuse, any bystanders, other children involved, staff and the wider school community;
- preserving evidence where appropriate and safe to do so;
- considering whether external advice, referral or reporting is required, including to children's social care, the police, the Local Authority Designated Officer, the National Crime Agency's CEOP reporting route, or other relevant agencies depending on the nature of the concern;
- addressing harmful behaviour through safeguarding, pastoral, behaviour and disciplinary procedures as appropriate;
- communicating with parents and carers where appropriate and where this does not increase risk to a child or compromise an investigation;
- reviewing the plan developed to address online abuse at regular intervals to ensure that any problems have been resolved in the long term and that further preventative action is considered.

### Guidelines on the use of AI

- AI tools, including generative AI, must be used safely, transparently, ethically and in line with safeguarding, data protection, confidentiality, intellectual property and academic integrity expectations.
- AI tools must be used under appropriate adult supervision and for educational or administrative purposes only.
- Staff must assess whether AI tools are age-appropriate, secure and suitable before use with pupils.
- Staff must check relevant age limits, terms of service, privacy arrangements and safeguarding risks before adopting AI tools.
- Personal, confidential, sensitive or safeguarding information must not be entered into AI tools unless the tool has been approved for that purpose and appropriate safeguards are in place.
- Staff should consider whether a Data Protection Impact Assessment is needed before introducing new AI tools or systems.
- Pupils must understand that AI-generated content may be inaccurate, biased, misleading or incomplete and should not be relied upon without appropriate checking.

- AI-generated content should be clearly identified where it is used in school work or communication.
- Pupils must not use AI to deceive, plagiarise, impersonate others, create harmful content, bully, harass, manipulate images, create deepfakes or compromise the dignity or safety of others.
- Staff must follow school guidance before using AI to support teaching, assessment, communication or administrative work.
- AI use must respect privacy, intellectual property rights, equality, dignity and the rights of others.
- The school will review AI use regularly to ensure it remains ethical, safe, proportionate and beneficial to pupils.
- Any concern involving AI-generated harmful content, impersonation, deepfakes, inappropriate image generation, harmful advice, grooming, bullying, harassment or misuse of pupil or staff data must be reported in accordance with safeguarding and data protection procedures.

### Statement on Pupils with SEND

The school recognises that pupils with SEND may have an increased vulnerability to online risk, particularly those with language and communication difficulties, social communication difficulties, impulsivity, anxiety, dependency on technology or reduced ability to identify unsafe situations. Online safety education will be adapted where necessary to meet pupils' individual needs, and reasonable adjustments will be made to supervision, teaching, device use and reporting routes where appropriate. Staff should remain vigilant where pupils use a school digital device as their normal way of working and ensure devices are kept appropriately updated, managed, filtered and monitored with the support of the school's IT provider. Online safety should be considered as part of wider pastoral and safeguarding support for pupils with SEND.

### Communicating about Online Safety with Parents

Annual Online Safety workshops are run by [Childnet](#) for children of all ages and their parents/carers to promote the importance of online safety both in and outside school. The school also sends regular updates to parents in the weekly newsletter, the Cygnet, and in occasional advisory letters. These communications may include guidance on online behaviour, social media, gaming, mobile phones, parental controls, AI, harmful content, misinformation, cyber security and reporting concerns. The school will work with parents and carers to promote consistent expectations between home and school wherever possible.

### Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

Policy Name:  
 Policy Number:  
 Owner:  
 Dates of review:  
 Date of issue:  
 Date of latest next review:

Online Safety Policy  
 SHS B19  
 Bursar  
 July 26  
 Aug 2026  
 July 2027

- Acceptable Internet Use Policies for Pupils and for Staff
- Anti-bullying
- Behaviour for Learning
- Data Protection Policy
- Mobile Phone Acceptable Use Policy for Boarding Pupils
- Pupil Code of Conduct
- Privacy Policy
- Safeguarding Policy
- SEND Policy
- Searches Policy
- Staff Code of Conduct
- Staff Handbook
- Storage and Retention of Data Policy
- Taking, Storing and Using Images of Children Policy

### Contact details

#### Online Safety Co-ordinator

Name: Elizabeth Jacka

email: JackaE@st-hughs.co.uk

#### Designated Safeguarding Lead (DSL)

Name: Julia Veness

email: venessj@st-hughs.co.uk

#### NSPCC Helpline

0808 800 5000

Policy Name:  
Policy Number:  
Owner:  
Dates of review:  
Date of issue:  
Date of latest next review:

Online Safety Policy  
SHS B19  
Bursar  
July 26  
Aug 2026  
July 2027