



BURGESS HILL
— GIRLS —

Online Safety Policy - Whole School including EYFS

32

Responsible for Initiating Review of Policy	Designated Safeguarding Lead Team
Committee to Review	Welfare and Boarding Committee
Last Review Date	April 2026
Review Period	Annually
Approved by (Committee and Date)	Governing Body
Approved by Board of Governors	Welfare and Boarding Committee 27 th April 2026
Effective Date of Policy	April 2026
Next Review Date	April 2027
Related Policies	<ul style="list-style-type: none">• Safeguarding policy• Behaviour Policy• Low level concerns policy• Staff code of conduct• IT Code of conduct• ICT Acceptable Use Policy (AUP)• Digital Charter• Data protection and privacy notices• Mobile Phone Policy• Candidate Privacy notice• Photography policy• Searching screening and confiscation policy

POLICY STATEMENT:

Burgess Hill Girls recognises that online safety is an integral part of safeguarding and child protection. The school is committed to ensuring that all members of the school community are protected from harm when using the internet, digital technologies and online platforms.

This policy reflects statutory guidance including Keeping Children Safe in Education (KCSIE), The Early Years Foundation Stage (EYFE) Statutory framework, Working Together to Safeguard Children, and the UKCIS guidance (including sharing nudes and semi-nudes), data protection legislation and the DfE Filtering and Monitoring Standards, (including DfE guidance on generative AI and product safety).

Independent School Standards Regulations

This policy supports the school's compliance with the Independent School Standards Regulations 2014, in particular Part 3 – Welfare, Health and Safety of Pupils, including the requirements to safeguard and promote the welfare of pupils and to protect them from harm, including online harm.

Online safety arrangements form a key part of the school's safeguarding framework and are implemented in conjunction with the Safeguarding (Child Protection) Policy and related procedures.

The welfare and safety of students is paramount, and online safety concerns are treated as safeguarding matters.

DESIGNATED SAFEGUARDING ROLES:

- **Designated Safeguarding Lead is:** Suzanne Roberts
- **Deputy DSLs:** Nicola Donson, Sue Collins, Iain Regan-Smith, Nicole Parker

The DSL has lead responsibility for safeguarding and child protection, including online safety.

The Governing body has appointed a safeguarding governor who receives appropriate training and has oversight of safeguarding arrangements, including online safety. They can be contacted via the Clerk to the governors at: dfo@burgesshillgirls.com

THE PURPOSE OF THE POLICY:

- Safeguard and protect all members of the school community online
- Educate pupils, staff and parents about online risks and safe behaviours
- Enable staff to work safely, responsibly and professionally online
- Provide clear procedures for responding to online safety concerns

CATAGORIES OF ONLINE RISK:

Online safety risks are categorised as:

- Content: exposure to illegal, inappropriate or harmful material, including pornography, violence, extremism, self-harm, suicide, misogyny, racism, antisemitism, misinformation and AI-generated or manipulated content.
- Contact: harmful interaction with others, including bullying, coercion, grooming, exploitation, or exposure to commercial pressure.
- Conduct: behaviours that increase harm, including cyberbullying, harassment, or the creation/sharing of sexual imagery.
- Commerce: risks such as financial scams, phishing, gambling, or inappropriate advertising.

ONLINE SAFETY AND THE PREVENT DUTY:

- Extremist content and online radicalisation are recognised as safeguarding risks.
- The school has a duty to prevent pupils from being drawn into extremism or terrorism (Prevent Duty).
- Any online concerns relating to extremist views or radicalisation must be treated as safeguarding issues.
- Concerns must be reported in line with safeguarding procedures and local guidance.
- Staff are trained to recognise signs of online radicalisation and extremism.
- All concerns must be shared with the Designated Safeguarding Lead (DSL), who will take appropriate next steps.

SCOPE:

This policy applies to:

- All staff, volunteers, governors, contractors and visitors
- All pupils from EYFS to Sixth Form
- All use of internet-enabled technologies, both on site and off site, including personal and school-issued devices

ROLES AND RESPONSIBILITIES:

Governing Body

- Ensure compliance with safeguarding and online safety requirements
- Receive regular reports on online safety incidents and trends
- Oversee filtering and monitoring arrangements

Senior Leadership Team

- Embed online safety as a safeguarding priority
- Ensure appropriate filtering and monitoring systems are in place
- Support the DSL with resources and training
- Ensure online safety is embedded within the curriculum

Designated Safeguarding Lead

- Act as the lead contact for all online safety concerns
- Maintain safeguarding records and oversee referrals
- Ensure staff training is up to date
- Liaise with external agencies where required

All Staff

- Model safe and professional online behaviour
- Identify and report online safety concerns immediately
- Follow all relevant policies and procedures

Pupils

- Use technology safely and responsibly
- Follow acceptable use agreements
- Report concerns to a trusted adult

Parents and Carers

- Support the school's online safety expectations
- Reinforce safe behaviours at home
- Raise concerns with the school promptly

Vulnerable Pupils

- Burgess Hill Girls is aware that some people are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) Or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Burgess Hill Girls will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
- Burgess Hill Girls will seek input from specialist staff as appropriate, including the SENDCO.

FILTERING AND MONITORING:

The school implements age-appropriate filtering and monitoring to reduce exposure to harmful content and identify potential safeguarding concerns.

The school acknowledges that:

- Filtering and monitoring cannot identify or prevent all risks
- Systems support, but do not replace supervision, education and professional judgement

Filtering and monitoring arrangements are:

- Risk assessed
- Reviewed regularly
- Logged and monitored by the DSL team, senior leaders and governors

The IT Manager maintains a clear log of all firewall checks, which are completed half termly. The DSL team are updated on any changes. The IT Manager records all actions taken in response to the filtering reports generated and any staff filtering requests which are raised. This not only ensures transparency and a robust evidence trail it also ensures that any potential safeguarding concerns are reviewed promptly and appropriately, and that safeguarding processes are followed consistently.

ARTIFICIAL INTELLIGENCE (AI) AND EMERGING TECHNOLOGY RISKS:

The school recognises that AI technologies present both educational opportunities and emerging safeguarding risks.

Risks include:

- AI-generated or manipulated content (e.g. deepfakes)
- AI-generated sexual imagery involving children
- Impersonation, grooming or automated abuse
- Misinformation and disinformation

https://assets.publishing.service.gov.uk/media/68add931969253904d155860/Keeping_children_safe_in_education_from_1_September_2025.pdf page 38, online safety - point 135.

SAFEGUARDING RESPONSE:

The school adopts a layered approach including education, staff vigilance, filtering and monitoring (where possible), and clear reporting pathways.

Concerns involving AI-enabled harm are treated as safeguarding issues and may be referred to external agencies including CEOP or the police.

Staff must risk assess AI tools before use and use them in line with professional standards and safeguarding principles.

EDUCATION AND TRAINING:

Pupils

- Online safety is embedded within PSHE, RSE and Computing
- Content is progressive and age appropriate
- Pupils are taught to think critically, seek consent and report concerns

Staff

- Online safety training is provided on induction and at least annually
- Training includes AI risks, filtering and monitoring, and professional conduct

Parents

- Information and guidance is shared through events, communications and the school website

RESPONDING TO ONLINE SAFETY CONCERNS:

All online safety concerns are treated as safeguarding matters and managed in line with the Safeguarding (Child Protection) Policy.

Where appropriate, concerns may be referred to:

- Local Authority Safeguarding Team
- Police (101/999)
- (Child Exploitation & online Protection) CEOP
- Internet Watch Foundation

Parents and carers will be informed unless this places a child at further risk.

SEARCHING, SCREENING AND CONFISCATION:

- As part of an online safety or safeguarding response, the school may need to search, screen, or confiscate a pupil's device or access digital content.
- Any action taken will be lawful, proportionate, and in line with the Searching, Screening and Confiscation Policy.
- Safeguarding, data protection, and pupil welfare are prioritised at all times.
- Decisions to search or access digital content are authorised by the Headteacher and/or Designated Safeguarding Lead (DSL).

- All relevant actions and decisions are recorded appropriately.
- Where illegal content is suspected, concerns are referred to the appropriate external agencies

MONITORING AND REVIEW:

This policy is reviewed annually, and earlier if:

- Statutory guidance changes
- New safeguarding risks emerge
- Significant incidents occur

Monitoring outcomes inform curriculum development, staff training and policy review.

USEFUL CONTACTS AND RESOURCES:

- NSPCC Online Safety: www.nspcc.org.uk/onlinesafety
- CEOP: www.thinkuknow.co.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Internet Watch Foundation: www.iwf.org.uk
- [Keeping Children Safe in Education \(KCSIE Sept 2025\)](#)
- [Early Years Foundation Stage Statutory Guidance \(EYFS Sept 25\)](#)
- [UK CIS sharing nudes and semi nudes' advice for Education settings](#)
- [gov.uk -guidance meeting digital and technological, filtering-and-monitoring core standards](#)
- [gov.uk government publications generative AI product safety Standards generative AI product safety standards](#)
- Let's Talk About It Provides advice for parents and carers to keep children safe from online radicalization
- Lucy Faithfull Foundation www.lucyfaithfull.org Including Stopnow resources – concerns about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- Parent Zone www.parentzone.org.uk provides help for parents and carers on how to keep their children safe online