BURGESS HILL GIRLS

Online Safety Policy - Whole School including EYFS	32

Responsible for Initiating Review of Policy	Designated Safeguarding Lead Team
Committee to Review	Boarding and Welfare
Last Review Date	June 2025
Review Period	Annually
Approved by (Committee and Date)	Governing Body
Approved by Board of Governors	
Effective Date of Policy	June 2025
Next Review Date	February 2026 (in line with Safer Internet Day which is 10th Feb 2026)
Related Policies	Behaviour Policy Safeguarding policy Low level concerns policy KCSIE IT Code of Conduct Acceptable Use Policy Digital Charter

Burgess Hill Girls takes the issues of online safety as an extremely important part of our safeguarding duties. This policy takes into account the DfE statutory guidance Keeping Children Safe in Education 2024, EYFS statutory framework 2024, and the UK CIS Sharing nudes and semi-nudes advice for education settings working with children and young people. GET LINKS

The Designated Safeguarding Lead is: Suzanne Roberts.
The Deputy Designated Safeguarding Leads (DSLs) are:

- Nicola Donson
- Sue Collins
- Iain Regan-Smith
- Nicole Parker

The Designated Safeguarding Lead (DSL) takes lead responsibility for safeguarding and child protection (including online safety).

The Governing body has nominated Miss Beth Gavin who has received appropriate training as the lead governor to take leadership responsibility for the schools safeguarding arrangements, including online safety. She can be contacted via the Clerk to the governors at: dfo@burgesshillgirls.com

- The purpose of the online safety policy is to:
  - safeguard and protect all members of Burgess Hill Girls community online.
  - identify approaches to educate and raise awareness of online safety throughout the community
  - enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards in practise when using technology.
  - Identify clear procedures to use when responding to online safety concerns.

- Burgess Hill Girls identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
  - Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
  - Contact: being subjected to harmful online interaction with other users; for example, 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; for example, 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. It is if it is felt that our students or staff are at risk we will report it to the Anti-Phishing Working Group.

Policy Scope

Burgess Hill Girls believes that online safety is an essential part of safeguarding, and we acknowledge our duty to ensure that all pupils and staff are protected from potential harm online.

- Burgess Hill Girls identifies that the Internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Burgess Hill Girls believes that staff and students should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.
- This policy applies to all access to the Internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school-issued devices for use off-site, such as a work device or mobile phones.

Links with other Policies and Practices

This policy links with other school policies, practices and action plans including:

- anti bullying
- data protection
- photography and recorded images
- privacy notice
- behaviour policy
- PSHE
- relationships and sex education
- safeguarding (child protection)
- staff privacy notice
- searching screening and confiscation
- staff code of conduct

The policy also takes into account 'The use of social media for online radicalisation (July 2015); sexual violence and sexual harassment between children in schools and colleges guidance in KCSIE; guidance from the UK Council for Child Internet Safety (UKCCIS), Sharing Nudes and semi-nudes: advice for education settings working with children and young people KCSIE 2024 and working together to safeguard children 2023, the Early Years Foundation Stage Statutory

Framework (2023) and GDPR 2018, and the DfE guidance: *Cyber-bullying: Advice for headteachers and school staff* (2014) and *Advice for Parents and Carers on Cyber-bullying* (2014).

Monitoring and Review

- This policy will be reviewed at least annually. The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- We will ensure that we regularly monitor Internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Head will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

Roles and Responsibilities

The Designated Safeguarding Lead, Suzanne Roberts, is responsible for online safety with the support of the Deputy Designated Safeguarding Leads.

Burgess Hill Girls recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The school will adopt a zero-tolerance approach to any cyber-bullying issues as per the anti-bullying policy. All staff will challenge any abusive behaviour between peers that comes to their notice and will report these issues to the DSL immediately. Please see the safeguarding policy for further details about responding to child-on-child abuse.

The Senior Leadership Team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements
- Ensure there are appropriate and up-to-date policies regarding online safety, including an IT Code of Conduct and an Acceptable Use Policy which covers acceptable use of technology
- Ensure that suitable and appropriate filtering and monitoring systems are in place
- Work with the Network Manager and IT Team to monitor the safety and security of school systems and networks
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access

regarding online safety concerns, including internal, local and national support.

- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement.

The Designated Safeguarding Lead (DSL), or deputies in their absence, will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up to date and appropriate online safety training. This training will include understanding roles and responsibilities in relation to filtering and monitoring, in line with KCSIE.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate to outside agencies as well as the governing body.
- Work with the senior leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet at least termly with the Governor with the lead responsibility for safeguarding and online safety.
- The DSL will meet termly with the Director of Operations and the Network Manager to discuss any online issues and responses.

It is the responsibility of all members of staff to:

- Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline
- Contribute to the development of online safety policies
- Ensure that they use the school's Wi-Fi, rather than 3G/4G/5G for any school-based work.
- Read and adhere to the online safety policy
- Take responsibility for the security of school systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.

- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and senior leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures (including password policies and encryption) to ensure that the schools IT infrastructure/system is secure are not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the school's filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the senior leadership team.
- Report any filtering breaches to the DSL and senior leadership team, as well as, the school's Internet service provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches, are reported to the DSL, in accordance with the school's safeguarding procedures.

It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age-appropriate online safety education opportunities
- Ensure that they use the school's Wi-Fi rather than 3G/4G/5G whilst they are in school.
- Contribute to the development of online safety policies
- Read and adhere to the school's IT Code of Conduct
- Respect the feelings and rights of others both on and offline
- Take responsibility for keeping themselves and others safe online
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

It is the responsibility of parents and carers to:

- Read the school IT code of conduct and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety

issues with their children and reinforce appropriate, safe online behaviours at home.

- Role model safe and appropriate use of technology and social media.
- Abide by the school's Acceptable Use Policy. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school online safety policies.
- Use school systems, such as learning platforms, and other school network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.
- Adhere to only taking still or video photographic images of pupils in school or on school-organised activities with the prior consent of the school and then only in designated areas. Images taken must be for private use only. Recording and/or photographing other than for private use would require the consent of the other parents whose children may be captured on film. Without this consent, the data protection legislation would be breached.
- Informing the school if parents do not wish their children to be photographed or filmed and express this view in writing, so that their rights will be respected. Further detail is available in the school's Photography Policy.

Education and engagement with pupils

The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible Internet use amongst pupils by:

Ensuring education regarding safe and responsible use precedes Internet access.

- Including online safety in the PSHE, RSE and computing programmes of study, covering use both at school and at home. This will include 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).
- Reinforcing online safety messages whenever technology or the Internet is in use.
- Educating pupils in the effective use of the Internet to research, including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to be critically aware of the materials they read and show them how to validate information before accepting its accuracy.

The school will support pupils to read and understand the IT Code of Conduct in a way which suits their age and ability by:

- informing pupils that network and Internet use will be monitored for safety and security purposes and in accordance with legislation;
- displaying the school's Digital Charter and Acceptable Use posters in all rooms with Internet access;
- Rewarding positive use of technology by pupils
- Implementing appropriate peer education approaches including peer-to-peer training and presentations in assemblies and student time.
- Providing online safety education and training as part of the transition programme across key stages and when moving between schools
- Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support the school's internal online safety education approaches.

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 andability 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.

Training and Engagement with Staff
The school will:

- Provide and discuss the online safety policy (including specific reference to pupils in EYFS) with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. These will be included as part of existing safeguarding and child protection training and updates and also a separate stand-alone online course on induction.

This will cover the potential risks posed to pupils (Content, Contact, Conduct and Commerce) as well as our professional practice expectations:

- Make staff aware that school systems are monitored, and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance

with the school's policies and the staff code of conduct when accessing school systems and devices.

- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

Awareness and Engagement with Parents and Carers

- Burgess Hill Girls recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the Internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parents' evenings, transition events and through email.
    - Drawing their attention to the school online safety policy and expectations in letters, our prospectus and on our website.
    - Requesting that parents and carers read online safety information as part of joining our school.
    - Requiring them to read the school IT Code of Conduct and discuss its implications with their children.

Reducing Online Risks

- Burgess Hill Girls recognises that the Internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material in line with legal parameters.

- Due to the global and connected nature of the Internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.

- All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly highlighted through a variety of education and training approaches.

Safer Use of Technology

Classroom Use

Burgess Hill Girls Uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Microsoft 365 applications
- Email
- games consoles and other games-based technologies
- digital cameras webcams and video cameras
- all school owned devices will be used in accordance with the schools' guidelines for staff and pupils and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- The school will ensure that the use of Internet- derived materials, by staff and pupils, complies with copyright law and acknowledged the source of information.
- Supervision of pupils will be appropriate to their age and ability.

Early Years Foundation Stage and Key Stage 1

Children's access to the Internet will be by adult demonstration, with regular directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the children's age and ability.

Key Stage 2

- Children will use age-appropriate search engines, online tools and learning platforms.
- Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the children's age and ability.
- Children will cover aspects of online safety through the 6-week online safety module during computing lessons, using a scheme from Kapow.

Key Stage 3, 4, 5

- Pupils will be appropriately supervised when using technology, according to their ability and understanding.
- The school will balance pupils' ability to take part in age appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice.

Managing Internet Access

- the school will maintain a written record of users who are granted access to the schools' devices and systems.
- All staff, pupils and visitors will read and sign an AUP before being given access to the school computer system, IT resources or Internet.

Filtering and Monitoring Decision-Making

- Burgess Hill Girls governors and senior leadership team have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and senior leadership team are aware of the need to prevent 'over-blocking', as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the senior leadership team; all changes to the filtering policy are logged and recorded.
- The senior leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

Filtering and Monitoring

- The school uses next-generation firewall appliances designed to deliver robust network security, performance, blocking and filtering sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The school uses SENSO and Securus which report and monitor usage.
- The school filtering system blocks all sites on the Internet Watch Foundation list.
- The school ensures that our filtering policy is continually reviewed.

Dealing with Filtering Breaches

- The school has a clear procedure for reporting filtering breaches.
- If pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediately to a member of staff.

- The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead or deputy and/or IT Team.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies such as: the IWF, the Police or CEOP.

Monitoring

- The school will appropriately monitor Internet use on school owned or provided Internet enabled devices. This is achieved by the proactive monitoring service Securus.
- The school has a clear procedure for responding to concerns identified via monitoring approaches: Securus send incident reports to the Head and the Designated Safeguarding Team . Incidents of a concerning nature are added as new incidents on the school's safeguarding system MyConcern. At this stage, the MyConcern process is triggered, and the incident is resolved through this.

Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection Legislation.

Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly.
  - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific permission; portable media will be checked by an antivirus/malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar e-mail attachments.
  - Regularly checking files held on the school's network.
  - The appropriate use of user logins and passwords to access the school network.

- Specific user logins and passwords will be enforced for all but the youngest users.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Password Policy

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.
- From Year 3, all pupils are provided with their own unique username and private passwords to access school systems; peoples are responsible for keeping their password private.
- We require all users to:
  - use strong passwords for access into our system
  - always keep their password private; users must not share it with others or leave it where others can find it. (Prep pupils to share with Computing teachers.)
  - Not to log in as another user at any time.

Managing the Safety of the School Website

- the school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE)
- The school will ensure that our website complies with guidelines for publications including:
  - Accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
  - Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, e-mail and telephone number.
  - The administrator account for the school website will be secured with an appropriately strong password.
  - The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

Publishing Images and Videos Online

- The school will ensure that all images in videos shared online are used in accordance with the associated policies, including (but not limited to): the image use policy, data security, AUP, codes of conduct, social media and use of personal devices and mobile phones.

Managing Email

- Access to school e-mail systems will always take place in accordance with data protection legislation and in line with other school policies, including confidentiality, AUPs and Code of Conduct.
  - The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the e-mail provider.
  - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  - School e-mail addresses and other official contact details will not be used for setting up personal social media accounts.

- Members of the school community will immediately tell the designated safeguarding lead or deputies in their absence if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Excessive social e-mail use can interfere with teaching and learning and will be restricted; access to external personal e-mail accounts may be blocked in school.

Staff

- The use of personal e-mail addresses by staff for any official school business is not permitted. All members of staff are provided with a specific school e-mail address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents. Staff should consider response times that fit in with their time away from school and their family/personal commitments. Anything of an urgent nature should be escalated to a line manager/SLT for advice/action.

Pupils

- Pupils will use school provided e-mail accounts for educational purposes from Year 3.
- Pupils will sign an AUP and will receive education regarding safe and appropriate e-mail etiquette before access is permitted.

Educational Use of Video Conferencing and/or Webcams

Burgess Hill Girls recognise that the use of video conferencing Zoom / Microsoft Teams, live lessons or recordings can bring challenges but also a very wide range of learning benefits.

- Microsoft Teams or Zoom video conferencing contact details will not be posted publicly.
- Staff will ensure that external video conferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.

Users

- Parents and carers' consent will be obtained prior to people's taking part in video conferencing activities outside of school.
- People will ask permission from a teacher before making or answering a Microsoft Teams/Zoom call or message received in school from outside of the premises.
- External Zoom/Microsoft Teams meetings will be supervised appropriately, according to the pupils' age and ability. Teachers wishing to have an online meeting with students must be agreed in advance with the Head of Department and/or Assistant Head Academic.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to video conferencing administration areas or remote control pages.

- The unique login and password details for the video conferencing services such as Zoom meetings and conferences will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

Content

- When recording a video lesson, it should be made clear to all parties at the start of the lesson; the reason for the recording must be given and recorded material will be stored securely for a fixed period. Staff should remind pupils that they do not have to contribute to the discussion if they do not wish their voice to be recorded.
- If third party materials are included, the school will check that recording is permitted to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a video conference; if it is a non-school site, staff will check that the material they are delivering is appropriate for the class.

Management of Applications which Record Children's Progress

- The school uses ISAMS to track pupils' progress and share appropriate information with parents and carers.
- The Head is ultimately responsible for the security of any data or images held of children. As such, they will ensure that tracking systems are appropriately risk assessed prior to use, and that they are used in accordance with GDPR and data protection legislation.
- To safeguard data:
    - Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content.
    - School devices will be appropriately encrypted if taken off site to reduce the risk of a data security breach in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

Social Media Expectations

- The expectations regarding safe and responsible use of social media applies to all members of the Burgess Hill Girls community.
- The term social media may include (but is not limited to): blogs wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chat rooms and instant messenger.
- All members of the Burgess Hill Girls community are expected to engage in social media in a positive, safe and responsible manner, at all times.
    - All members of the Burgess Hill Girls community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on

any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

- The school will control pupil and staff access to social media whilst using school provided devices and systems on site.
    - The use of social media during school hours for personal use is permitted but only when it relates to school related business e.g. school blue sky and Instagram accounts.
    - Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.

- Concerns regarding the online conduct of any member of the Burgess Hill Girls community on social media, should be reported to the school and will be managed in accordance with that anti bullying, allegations against staff, behaviour and safeguarding (child protection) policies.

Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the Staff Code of Conduct.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves on their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites as strictly as they can.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use
    - keeping passwords safe and confidential
    - ensuring staff do not represent their personal views as that of the school
- Members of staff are encouraged not to identify themselves as employees of Burgess Hill Girls on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their

social media use is compatible with their professional role and is in accordance with the schools policies and the wider professional and legal framework.

- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the senior leadership team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and parents and carers

All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the Designated Safeguarding Lead (DSL) and/or the Head. If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks LinkedIN or use official school provided communication tools.

- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Head.
- Any communication from peoples and parents received on personal social media accounts will be reported to the school's Designated Safeguarding Lead.

Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils via the PSHE curriculum and as part of an embedded and progressive education approach, via age-appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create account specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Pupils will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples could include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends, family, specific interests and clubs.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.

- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications and report concerns both within school and externally.

Official Use of Social Media

- Burgess Hill Girls' official social media channels are Facebook, Instagram, TikTok and BlueSky.
- The official use of social media sites by the school only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  - The official use of social media as a communication tool has been formally risk assessed and approved by the Head.
  - Senior leadership staff have access to account information and login details for the social media channels, in case of emergency, such a staff absence.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
  - Staff use school provided e-mail addresses to register for and manage any official school social media channels. Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website.
  - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including anti bullying, image use, data protection, confidentiality, and safeguarding (child protection) policy.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents, carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
  - Social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
  - Any official social media activity involving pupils will be moderated by the school where possible.
- Parents and carers will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff Expectations

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.

- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
    - Be professional at all times and aware that they are an ambassador for the school
    - disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of the school.
    - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data Protection, and Equalities laws.
    - Ensure that they have appropriate written consent before posting images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
    - Inform their line manager, the Designated Safeguarding Lead (DSL), and/or the Head of any concerns, such as criticism, inappropriate content or contact from pupils.

Use of Personal Devices and Mobile Phones

Burgess Hill Girls recognise that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

Expectations

- All use of personal devices on mobile phones will take place in accordance with the law and other appropriate school policies, including (but not limited to): anti bullying, behaviour and safeguarding (child protection), online safety policy.
- electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
    - All members of the Burgess Hill Girls community our advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
    - All members of Burgess Hill Girls' community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the school site such as changing rooms, toilets and restricted use in the Nursery.

- The sending of abusive or inappropriate messages/content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- Old members of Burgess Hill Girls' community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school behaviour or safeguarding (child protection) policies.

Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as relevant school policy and procedures such as: confidentiality, safeguarding (child protection), data security and AUP.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time
    - keep mobile phones and personal devices switched off or switch to silent mode during lesson times
    - ensure that Bluetooth or other forms of communication (such as 'Air Drop') are hidden or disabled during lesson time.
    - Not to use personal devices during teaching periods, unless written permission has been given by the Head.
    - Ensure that any content brought onto site via mobile phones and personal devices is compatible with their professional role and expectations.
    - Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - Any pre-existing relationships which could undermine this, will be discussed with the Designated Safeguarding Lead (DSL) and/or Head.
- Staff will not use personal or school cameras (digital or otherwise) or camera phones for taking and transferring images of pupils or staff without permission from SLT. Photographs of pupils must not be stored at home. School camera memory card should be downloaded onto school computers only. Personal memory cards should never be put into school cameras, and school memory cards should never be put into personal cameras. Where permission has been granted to use a personal device, the transfer of images must take place on site as soon as is practicable after the event and within one calendar week. Should any member of staff become aware of inappropriate or non-essential use of camera phones, including iPad, devices and cameras, this should be reported to a member of SLT. In addition, for EYFS, photographs will be taken for the purpose of recording a child or group of children participating in activities of celebrating their achievements and in an effective way to record their progress in development. All such images will be appropriately stored on school equipment.
- If a member of staff breaches the school policy, action will be taken in line with the school disciplinary policy.

- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

Pupils' Use of Personal Devices and Mobile Phones

- People will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Burgess Hill Girls expects pupils' personal devices and mobile phones to be switched off during their time at school. If a pupil needs to contact their parents or carers they will be allowed to use the school office phone. Pupils in the Prep School who bring a mobile phone to school (if permission has been given) have to give their phone in to the school office when they arrive and collect it at the end of the day.
- Parents are advised to contact their child via the school office during school hours; exceptions may be permitted on a case-by-case basis, as approved by the Head.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time and less as part of an approved and erected curriculum-based activity with consent from a member of staff.
    - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
    - If during lessons peoples are allowed access to their mobile phones, this should be under the guidance of their teacher. They should not use mobile data but should instead use the school's Wi-Fi.
- Mobile phones and personal devices including watches must not be taken into examinations.
- People found in possession of a mobile phone or personal device during an examination will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches the school policy, the final device will be confiscated and will be held in a secure place.
    - School staff may confiscate a people's mobile phone or device if they believe it is being used to contravene the school's behaviour or anti bullying policy, or could contain indecent images, shared either consensually or non-consensually, has been used to view and share pornography, or has evidence of sexual harassment of peers or other harmful content.
    - Searches of mobile phone or personal devices will only be carried out in accordance with the school's policy which has been written using the DfE advice: https://www.gov.uk/government/publications/searching-screening-and-confiscation

- People's mobile phones or devices may be searched by a member of the senior leadership team, with the consent of the pupil or a parent/carer. Content may be deleted or requested to be deleted, if it contravenes school policies.
- Mobile phones and devices that have been confiscated will usually be released to parents or carers at the end of the day.
- If there is suspicion that material on the people's personal device or mobile phone may be illegal or may provide evidence related to a criminal offence, the device will be handed over to the police for further investigation.

Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's acceptable use policy and other associated policies, suchas: anti bullying, behaviour, safeguarding (child protection) policy and image use. Visiting speakers will follow the protocols in the visiting speaker risk assessment and guidance. Only the school's guest Wi-Fi may be used.
- The school will ensure appropriate signage and information is displayed/provided to inform parents carers and visitors have expectations of use. Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.
- Parents, carers or relatives may only take still or video photographic images roles in school or on school-organised activities with the prior consent of the school and then only in designated areas. Images taken must be for private use only. Recording and/or photographing other than for private use would require the consent of the other parents whose children may be captured on film. Without this consent, the Data Protection Legislation would be breached. If parents do not wish their children to be photographed or filmed and expressed this view in writing, their rights will be respected. Further detail is available in the school's photography and recording images policy.

Officially Provided Mobile Phones and Devices

- Members of staff will be issued with a work phone number and e-mail address, where contact with parents/carers is required.
- School mobile phones and devices will be suitably protected via passcode/password/pin and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies including the safeguarding (child protection) policy.

Responding to Online Safety Incidents and Concerns

The school will treat concerns relating to online incidents as a safeguarding risk and the school's safeguarding (child protection) policy will be followed.

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual imagery, cyber bullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
- Pupils, parents and staff will be informed at the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learned and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL or DDSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion, that illegal activity has taken place, the school will contact the education safeguarding team or police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with the police and/or the education safeguarding team first, to ensure that potential investigations are not compromised.

Concerns about Pupils' Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL will record these issues in line with the school's child protection policy
- the DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the local authority thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

Staff Misuse

- Any complaint about staff misuse will be referred to the Head according to the safeguarding policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the behaviour policy and staff code of conduct.

If the school are made aware of an incident involving online sexual abuse of a child, the school will act in accordance with the school's safeguarding policies (child protection) and the relevant Local Authority Safeguarding Children Partnership procedures.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Burgess Hill Girls.

- As required by KCSIE, appropriate filtering and monitoring systems are in place, and any concerns flagged by the systems are followed up by the pastoral team.
- Full details of how the school will respond to cyberbullying are set out in the anti-bullying policy.

Artificial Intelligence (AI)

- generative AI tools are now widespread and easy to access. Burgess Hill Girls recognises that AI has many potential uses to help pupils learn but also may be used to bully others.
- AI can be used in the form of 'deepfakes', where images, videos or audio hoaxes are created that look real. This includes deep fake pornography, created using AI to include someone's likeness.
- Burgess Hill Girls will treat any use of AI to bully pupils in line with our anti bullying policy.
- Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used.

Online Hate

- online hate content, directed towards or posted by a specific members of the community will not be tolerated at Burgess Hill Girls and will be responded to in line with existing school policies, including anti bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or the police.

Online Radicalisation and Extremism

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the Internet in school.

- The school recognises its Prevent Duties and associated response should there be any concern that a child is vulnerable to radicalisation and extremism. This is informed in part by the school's Prevent risk assessment, working hand in hand with the West Sussex Prevent Team.
- Is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately, and action will be taken in line with the safeguarding (Child Protection) Policy.
- If the school is concerned that a member of staff may be at risk of radicalisation online, the Head will be informed immediately, and action will be taken in line with the Safeguarding (Child Protection) and Whistleblowing policies.

Responding to an Online Safety Concern

Training

Staff will attend regular training to keep up to date with latest online safety guidelines the following are not permissible when working with or on school hardware or software:

- the deliberate uploading, downloading, sending, viewing or publishing of material that is inappropriate in a school environment, offends common decency or members of staff or pupils or visitors to the school, violates the laws of the land or is against the rules and conditions of Burgess Hill Girls' Internet service provider. This includes but is not limited to pornographic material, graphical or textural or offensive language or extreme political or religious views or material promoting terrorist activity or homophobic or racist or sexist material.
- The use of chat rooms or discussion forums or similar interactive services for non-school related matters. Whether the use is school-related shall be determined by the Head or the Director of Finance and Operations.
- The duplication and/or publication by any means, including email, storage device copies or publication on a website, of any information held within the school that is private, confidential or sensitive.
- The publication of any material which could be considered as slanderous or libellous or likely to damage the reputation of the school. 'Publication' includes saving to storage device and/or printing.
- The setting up or administration or running of any business activity, club society or other non-profit venture not directly related to the school's affairs, without the prior written approval of the Head or the Director of Finance and Operations.

The illegal copying of software, including:

- Computer programs and data
- Music and video or photographic material, staff should note that various arrangements are available for the purchase at discounted rates of software for home use. Colleagues should refer to the IT team for guidance in the first instance.
- The unauthorised dismantling or modification of hardware, or the removal of parts from a system.
- The deliberate misrepresentation of school matters or school policy in any form including by email, contributions to newsgroups, setting up or contributing to websites, or contributions to guestbook services.
- The use of school equipment (other than school laptops) out of normal school hours for personal use without the prior approval of the Head or Director of Finance and Operations.
- The sending or forwarding of any virus internally or externally, or the deliberate failure to report the known existence of a virus within the school, thus preventing its spread. The sending or forwarding of any communication about a hoax with the intention of misleading other members of the school.
- The giving of password or other security information that would allow unauthorised users to view sensitive or confidential information, or make unauthorised changes to information, for example, on any school database or the

school's website. Do you care is to be taken to ensure that offices containing hardware linked to the internal network are not left unattended and unlocked, as this gives opportunity for our authorised access to the system. Passwords should not be divulged, should be changed frequently, be of sufficient complexity, and should be changed immediately if there is any likelihood of the password having been compromised.

- The excessive use of private email services. While the school respects the privacy of staff, where there is reason for concern, the school reserves the right to monitor and intercept e-mail communications.
- The sending of an email representing the school without the appropriate and official school legal disclaimer attached – any email communication must not bring the school into disrepute.
- The use of school equipment to the detriment or exclusion of normal school responsibilities.
- The creation of or contribution (including the uploading of pictures) to any website which makes unsubstantiated, anonymous, defamatory or otherwise unacceptable comments about any member of the school community, all the school policy, or any aspect of the running of the school, or the failure to report the existence of any such known sight to the Head or Director of Finance and Operations.
- The failure to report to the Head or Director of Finance and Operations any known transgression of any of the above rules by any other member of staff. This may be made in confidence. Any concerns relating to safeguarding, child protection and online safety issues should be reported to the Designated Safeguarding Lead.

Staff may give permission for peoples to borrow laptops (or similar) for use on schoolwork at home at their discretion, in which case the full record should be kept, unsuitable arrangements made for its return.

All Internet use is logged for the purposes of maintaining standards of security and acceptable use, and the school reserves the right to monitor its use.

For the avoidance of doubt, it should be noted that staff are bound by current relevant legislation, details of which are maintained by the Director of Finance and Operations, and which will be made available to staff upon request. Serious breaches of this policy may result in procedures being invoked under the school's disciplinary policy.

Useful Links for Educational Settings
Police:

- In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent inquiries contact the police via 101.
- Beverly Knight - Prevent Lead – West Sussex Beverly.knight@westsussex.gov.uk

National Links and Resources

- Action Fraud
- CEOP
- ChildLine
- www.thinkuknow.co.uk
- www.childnet.com
- www.getsafeonline.org
- Internet Matters www.internetmatters.org
- Internet Watch Foundation www.IWF.org.uk
- Let's Talk About It Provides advice for parents and carers to keep children safe from online radicalisation.
- 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)
- NSPCC www.nspcc.org.uk/onlinesafety
- NEW dedicated NSPCC helpline 0800 136 663
- Net Aware www.net-aware.org.uk
- Parent Zone www.parentzone.org.uk provides help for parents and carers on how to keep their children safe online
- The Marie Collins Foundation www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline www.saferinternet.org.uk/about/helpline
- 360 Safe Self-review tool for schools: www.360safe.org.uk

APPENDIX 1: IT Code of Conduct – Senior School
APPENDIX 2: ICT Acceptable Use Agreement