BLACKHEATH HIGH SCHOOL

GDST

Online Safety Policy

POLICY INDEX

Page	Contents
2	Policy Introduction and Aims
2	Policy Scope
3	Roles and Responsibilities
6	Education and Engagement
8	Reducing Online Risks
8	Safer Use of Technology
10	Social Media
11	Reporting & responding to Online Incidents and Concerns
12	Monitoring and Review
12	Useful links and sources of advice
14	Appendix 1 – Guided home learning and live online teaching
17	Appendix 2 - Use of Personal Devices and Mobile Phones

Person responsible:	JL/GDST
Contact details of person responsible:	j.leamon@bla.gdst.net
Identified Governor:	N/A
Reviewed by and frequency:	Annually by JL/GDST
Date of last review:	September 2026
Policy approved by SLT on:	September 2026
Date of next review:	September 2027

GDST Online Safety Policy

September 2026

1. Policy Introduction and Aims

The internet and associated devices, such as computers, tablets, mobile phones, wearable tech and games consoles, are an important part of everyday life. However, these modern technologies have created a landscape of challenges and dangers that is constantly changing. In order to ensure that the school provides a safe environment for learning, we adhere to the following principles:

- Online safety is an essential part of safeguarding, and the school has a duty to ensure that all pupils and staff are protected from potential harm online.
- Online safety education is an important preparation for life. Pupils should be empowered to build resilience and to develop strategies to prevent, manage and respond to risk online.

The purpose of the online safety policy is to:

- Safeguard and protect all members of the school's community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Set expectations for safe, responsible, professional and ethical use of technology (including generative artificial intelligence).
- Identify clear procedures to use when responding to online safety concerns.

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, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact:** being subjected to harmful online interaction with other users or generative artificial intelligence (AI) applications that simulate this; 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:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g. consensual and non-consensual making or sharing of nudes and semi-nudes, including those generated using AI e.g. deepfakes), sharing other explicit images and online bullying, and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Policy Scope

This policy applies to all staff including teachers, trainee 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. It applies to the whole school including the Early Years Foundation Stage. It applies to access to school systems, the internet, and the use of technology, using devices provided by the school or personal devices.

The policy also applies to online safety behaviour such as cyber-bullying, which may take place outside the school, but is linked to membership of the school. The school will deal with such behaviour within this policy and associated behaviour and discipline policies, and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

2.1 Links with other policies and practices

This policy links with a number of other policies, procedures and guidance documents including:

- The GDST *Information Security Policy*
- The GDST *Data Protection Policy*
- The GDST Filtering and Monitoring Procedure
- The school's *Safeguarding and Child Protection Policy*
- The GDST *School Staff Code of Conduct*
- *Acceptable Use Agreements* (AUAs) for staff and pupils
- The GDST *Social Media Policy*
- GDST Use of student imagery guidance for schools
- The school's *Behaviour and Reward Policy*
- The school's Unkindness and *Anti-Bullying Policy*

3. Roles and Responsibilities

3.1 GDST Safeguarding Committee

The Safeguarding Committee is responsible for reviewing and monitoring safeguarding law, policy, guidance and GDST safeguarding policies and procedures, which includes this policy. The Safeguarding Committee is responsible for ensuring the GDST Council is kept appropriately informed of safeguarding issues and that safeguarding considerations form part of discussions at Council and its committees as appropriate. The role of the Safeguarding Committee is to:

- Minimise the risk of harm to pupils, promote the welfare of pupils, and to protect pupils and staff.
- Promote and ensure best practice in safeguarding across all GDST schools and academies.
- Oversee the monitoring and review of the effectiveness and implementation of GDST's safeguarding policies and procedures.
- Monitor changes in legislation, policy and government guidance, help coordinate further action and minimise the risk of non-compliance with respect to ISI and Ofsted inspections.
- Coordinate the work of Trust Office departments responsible for aspects of safeguarding, and to facilitate liaison between Trust Office and schools.
- To report on safeguarding oversight and policy changes to the Education and People Committee, and, where appropriate, to make recommendations regarding changes or developments to policy or practice to the Executive Board.

The Safeguarding Committee is responsible for ensuring that online safety practice is audited and evaluated regularly and that the GDST employs a filtering and monitoring provision that complies with the statutory requirements, set out in *Keeping Children Safe in Education* (KCSIE) and the Prevent Duty which is designed to safeguard against harmful and illegal content, including child sexual abuse material (CSAM), and support the well-being of our school community.

3.2 GDST Online Safety Group

The Online Safety Group brings together relevant Trust Office departments and school representatives to consider online safety developments and challenges, and how to address or manage these across the GDST network. The role of the group is to:

- Contribute to and review the online safety audit
- Review online safety issues raised to the Safeguarding Committee
- Consider schools' collective experience of online safety practice and possible improvements to centrally managed procedures
- Make recommendations to the Safeguarding Committee

3.3 School Governing Board

The School Governing Board has no formal responsibilities in relation to safeguarding, including online safety. However, as part of its role to satisfy itself that the school has a whole school approach to safeguarding and that all school systems, processes and policies operate with the best interests of the child at their heart, the SGB should be kept informed of online safety policy and practice via the termly SGB Safeguarding Report.

3.4 The Head:

- Has overall responsibility for online safety provision in school.
- Ensures that online safety is viewed as a safeguarding issue and that practice is in line with GDST and national recommendations and requirements.
- Ensures the school follows GDST policies and practices regarding online safety (including the IT *Acceptable Use Agreements*), information security and data protection.
- Determines the school's internal policy on the use of personal devices (including wearable tech) and mobile phones.
- Ensures that online safety is embedded within the whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Supports the DSL by ensuring they have sufficient training, time, support and resources to fulfil their responsibilities.
- Ensures that all staff receive regular, up to date and appropriate online safety training.
- Is aware of what to do in the event of a serious online safety incident and will ensure that there are robust reporting channels for online safety concerns, including internal, GDST and national support.
- Receives regular reports from the DSL on online safety.

3.5 The Designated Safeguarding Lead (DSL):

- Takes day to day responsibility for online safety in school.
- Maintains an up-to-date knowledge of online risks, including filtering/monitoring platforms and processes, cyber security, wearable tech and similar emerging technologies, and AI-related safeguarding risks
- Promotes an awareness of and commitment to online safety throughout the school community.

- Acts as the named point of contact on all online safety concerns and issues, coordinates the response and records, escalates and refers such incidents in line with safeguarding procedures. .
- Keeps the online safety component of the curriculum under review, in order to ensure that it remains up to date and relevant to all pupils, including those with SEND.
- Facilitates training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the school community, as appropriate.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- Reviews and responds to alerts generated by the GDST filtering and monitoring solution, or other incidents of online behaviour that may indicate a safeguarding concern.
- Reports regularly to the Head and SLT on matters of online safety, current issues, developments in legislation etc.
- Where pupils are taught through cross-school programmes such as ConnectEd, ensures that appropriate arrangements are in place for the sharing, review and escalation of relevant pastoral, attendance and safeguarding information, and that staff understand how to access support and report concerns.

3.6 Staff managing the technical environment:

- Apply appropriate technical and procedural controls to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Keep up to date with the *Online Safety Policy* and technical information in order to carry out their online safety role effectively and to inform and update others as relevant.
- Provide technical support to the DSL and leadership team in the implementation of online safety procedures.
- Ensure that the school's filtering rules and policies are applied; support the DSL on a regular basis to review filtering rules and changes; and ensure that the school's monitoring systems are operational.

3.7 All school staff:

- Read, adhere to and help promote the *Online Safety Policy*, IT *Acceptable Use Agreements* and other relevant school policies and guidance.
- Take responsibility for the security of school systems and the data they use or have access to.
- Model safe, responsible, and professional behaviours in their own use of technology.
- Embed online safety in their teaching and other school activities.
- Supervise, guide, and monitor pupils carefully when engaged in activities involving online technology (including extra-curricular and extended school activities if relevant).
- Have an up-to-date awareness 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 reporting to the DSL.
- Know when and how to escalate online safety issues.
- Take personal responsibility for professional development in this area.

3.8 Pupils (at a level that is appropriate to their individual age, ability and vulnerabilities):

- Engage in age-appropriate online safety education opportunities.

- Read and adhere to the school IT *Acceptable Use Agreements.*
- Respect the feelings and rights of others both on and offline, in and out of school.
- Take responsibility for keeping themselves and others safe online.
- Report to a trusted adult if there is a concern online or about the use of technology.
- Understand that out-of-school behaviour may be addressed where it affects the school community.

3.9 Parents and carers:

- Read the school *Acceptable Use Agreements* and encourage their children to adhere to them.
- Support the school in online safety approaches by discussing online safety issues with their children and reinforcing appropriate, safe online behaviours at home.
- Model safe and appropriate use of technology and social media, including seeking permission before taking and sharing digital images of pupils other than their own children.
- 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 or in their use of technology.
- Use school systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

4. Education and Engagement

4.1 Education and engagement with pupils

Online safety is a running and interrelated theme across the curriculum. The planned, progressive and inclusive programme is age-appropriate, builds on prior learning, and is matched to need. The aim is to raise awareness, build resilience, and promote safe and responsible internet and technology use by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety across the curriculum, including the Personal Social and Health Education, Relationships and Sex Education and Computing programmes of study, covering use both at school and home.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Ensuring that the needs of pupils considered to be more vulnerable online, such as those with SEND or mental health needs, are met appropriately.
- Using support, such as peer education approaches and external visitors, to complement online safety education in the curriculum.
- Developing pupils' ability to recognise and manage online risks, including harmful content, contact, conduct and commerce risks.
- Helping pupils to understand consent, online sexual harassment and sexual violence, supported by safe opportunities for discussion.
- 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 what they see online, including AI-generated content, and shown how to validate information before accepting its accuracy.
- Teaching pupils to respect and adhere to principles of academic integrity. This will include understanding the importance of producing their own independent work, being transparent and honest about any use of source material or AI-generated content, and respecting copyright and intellectual property.
- Teaching pupils in an age-appropriate way about the particular risks of generative AI platforms and other emerging technologies.
- Supporting students in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

The school will support pupils to read and understand the *IT Acceptable Use Agreement* in a way which suits their age and ability by:

- Discussing the IT AUA and its implications, and reinforcing the principles via display, classroom discussion etc.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Recognising positive use of technology by pupils.

4.2 Training and engagement with staff

The school will:

- Provide and discuss the *Online Safety Policy* and staff *IT Acceptable Use Agreement* 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.
- 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 school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media and other technologies, 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.

4.3 Awareness and engagement with parents and carers

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:

- Drawing parents' attention to the GDST *Online Safety Policy* and its expectations in newsletters and on the website
- Requiring parents to read the pupil *IT Acceptable Use Agreement* and discuss its implications with their children.

- Informing parents about what the school asks pupils to do online, and who they will be interacting with.
- 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 parent evenings.
- Supporting parents with establishing safe boundaries for their children around the use of technology such as mobile phones and platforms such as social media, in line with government guidance and legislation.

5. Reducing Online Risks

The internet is a constantly changing environment with new apps, devices, websites, and material emerging at a rapid pace. The school 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 technology use takes place within legal guidelines relating to safeguarding, data protection and intellectual property law.
- Ensure, through online safety education and the school IT Acceptable Use Agreements, that pupils know that the school's expectations regarding safe and appropriate behaviour online apply to both the school's networks and devices and personal internet connections and devices. The use of wearable devices, smart glasses, hidden cameras, AI-enabled recording devices or similar technologies capable of capturing images, audio or personal information without the knowledge of others is prohibited unless expressly authorised by the school.

6. Safer Use of Technology

The school uses a wide range of technology. This includes access to:

- Computers, laptops, and other digital devices
- Internet which may include search engines, AI and educational websites
- Learning platforms
- Cloud services and storage
- Email and messaging
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras
- Virtual reality headsets

The school is committed to ensuring that all technology used within the school environment is safe, secure, and appropriate for educational use. This includes both the provision of technology and the implementation of robust systems to manage and monitor its use.

- Supervision of pupils will be appropriate to their age and ability.
- All school-owned devices should be used in accordance with the school's ICT AUAs and with appropriate safety and security measures in place.
- Members of staff should always check websites, tools and apps for suitability before use in the classroom or recommending for use at home. Further information is provided in the GDST guidance on digital technology.

- Staff and pupils should consider copyright law and principles of academic integrity before using internet or AI derived materials (and where appropriate comply with licence terms and/or acknowledge the source of information).

6.1 Filtering and Monitoring

To safeguard pupils and staff from harmful or inappropriate online content, the school implements a comprehensive filtering and monitoring strategy that aligns with statutory requirements, including *Keeping Children Safe in Education* (KCSIE) and the Prevent Duty. This strategy is designed to:

- Prevent access to illegal, harmful, or inappropriate content, including child sexual abuse material (CSAM), extremist content, and other material that may pose a risk to wellbeing or safety.
- Monitor user activity on school devices and networks to detect potential safeguarding concerns, breaches of acceptable use, or indicators of risk.
- Support early intervention by alerting designated safeguarding staff to concerning behaviour or content, enabling timely and proportionate responses.

All school owned devices are subject to filtering and monitoring, including when used off site. Where the use of personal devices is allowed, users understand that their use may be filtered and monitored by the school.

Key elements of the filtering and monitoring provision include:

- GDST-managed filtering systems, which are safeguarding-led, proportionate and regularly reviewed (at least annually) and updated to reflect emerging threats and changes in online behaviour and checks to ensure that filtering is working appropriately on all internet-connected devices in all relevant locations, with a record kept of these checks.
- Active monitoring tools that provide real-time alerts to the Designated Safeguarding Lead (DSL) and relevant staff, enabling prompt investigation and action.
- Age-appropriate filtering rules, ensuring that pupils at different stages of education are protected while still able to access educational resources.
- Audit and oversight by the GDST Safeguarding Committee, which ensures that filtering and monitoring systems are effective, compliant, and proportionate.

6.2 Use of Generative Artificial Intelligence (AI)

AI is developing rapidly and its use in education and in wider society is increasing. We recognise that this presents both significant opportunities and safeguarding risks. Increasingly, AI is embedded in familiar tools, meaning that a previously approved digital tool may introduce new risks. AI can also be used in new and emerging wearable technology in a way which exposes the user and those around them to harm.

These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, by updating procedures where needed. Safeguarding of pupils and staff remains central to any use of AI.
Some AI-related risks are of particular relevance to safeguarding and pupil welfare, such as:

- Deepfakes, AI-generated child sexual abuse imagery, and grooming via avatars and chatbots
- AI-assisted extremist content

- Pupils developing an emotional attachment to chatbots which may become a substitute for human relationships and bypass trusted adult contact
- Cognitive offloading, which may reduce help-seeking from human sources and create conditions where disclosures are missed
- Discrimination and bias being amplified by AI outputs
- The amplification of risk for vulnerable pupils

When procuring and implementing AI systems and applications, we will follow due care and diligence to identify and mitigate these risks, using the guidance provided to schools by the Department for Education use.

- Comply with relevant law and guidance, including *Keeping Children Safe in Education* and data protection laws, and ensure the protection of personal and sensitive data and intellectual property. Personal, confidential or special category data may only be entered into AI systems where this is permitted under the GDST AI Policy.
- Risk-assess AI technologies before approving their use.
- Prioritise human oversight. AI may be used to assist but will not replace human decision-making. Any AI-generated content will be fact-checked and reviewed for accuracy before sharing or publishing.
- Provide training and guidance for staff on the benefits, risks and safe use of AI.
- Teach about AI through the curriculum where appropriate, helping pupils understand how AI works, its benefits, limitations and risks, and its ethical implications and social impacts.
- Ensure any safeguarding or wellbeing concern arising from AI use is fully investigated and reported if appropriate to external agencies such as children's social care and/or the police, in accordance with the procedures set out in the *Safeguarding and Child Protection Policy*.

7. Social Media

Social media is defined as any interactive online media that allows people to communicate with each other or to share ideas, opinions or data. This includes, but is not limited to, social forums such as Instagram, Tiktok, Facebook, LinkedIn, and X (formally known as Twitter), blog, livestream and video- and image-sharing websites such as YouTube, social communication apps such as WhatsApp, Snap, Telegram and Signal, and includes all other social networking sites and internet postings. It includes taking part in discussions on web forums or message boards and providing reviews on business or customer review websites.

7.1 Staff use of social media

Staff use of social media is governed by the GDST Social Media Policy.

7.2 Pupils' personal use of social media

School curricula are designed to provide a well-rounded education that goes beyond academic subjects and includes the development of social skills and pastoral support. Online services that support personal, social, health, peer support and extracurricular activities are considered to form part of this.

The use of social media will only be facilitated for students under the age of 16 where this is for the purpose of delivering the curriculum. Where the terms of service of a social media platform advise they are unsuitable for a child below a defined age, we will abide by these restrictions.

- Safe and appropriate use of social media will be taught to pupils as part of online safety education, via age-appropriate sites and resources.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

8. Reporting and Responding to Online Safety Incidents and Concerns

Schools are committed to creating a culture where all members of the community feel confident, safe and supported in reporting online safety concerns.

8.1 Reporting

- There are clear, accessible reporting routes in place for all members of the school community, including pupils, staff, parents and volunteers.
- Multiple reporting options are available, including speaking with the DSL or another member of staff, or email contact. These are well publicised through induction, assemblies, posters and digital platforms.
- Reporting processes are fully aligned with procedures for safeguarding, whistleblowing, managing allegations and complaints.
- All users understand that any online safety concern must be reported, including those related to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self/AI-generated nudes and semi-nudes.
- All reports will be acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.

8.2 Responding

- Incidents will be managed depending on their nature and severity, according to the relevant school policies
- Where an incident involves unauthorised access to, disclosure of, loss of, or misuse of personal information, it must be reported and managed in accordance with the GDST Data Protection Policy and Personal Data Breach procedures.
- A secure and confidential record will be kept of all incidents, including actions, decisions, and follow-up.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes in policy or practice as required.
- Reports will be analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the ITS or Legal Department at Trust Office.

8.3 Concerns about Pupils' Welfare

- The DSL will be informed immediately of any online safety incident that could be considered a safeguarding or child protection concern.
- The DSL will ensure that online safeguarding concerns are escalated and reported to relevant agencies.

- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

8.4 Misuse

- Complaints about technology misuse by pupils will be dealt with by a senior member of staff under the relevant policies and procedures and according to the nature of the complaint.
- Any complaint about staff misuse will be referred to the Head.
- Pupils and parents are informed of the school's complaints procedure.

9 Monitoring and Review

- The school will monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied in practice.
- The online safety policy framework will be reviewed by the GDST at least annually, and in response to any new national guidance or legislation, significant developments in the use of technology, emerging threats or incidents that have taken place.

10 Useful links and sources of advice

10.1 Guidance and resources

- Teaching Online Safety in School (DfE)
- Generative AI in education (DfE)
- Meeting digital and technology standards in schools and colleges (DfE)
- Education for a Connected World (UKCIS)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS)
- Professional Guides: Understanding and responding to AI-generated child sexual abuse material (IWF)
- Harmful online challenges and online hoaxes (DfE)
- Cyberbullying: understand, prevent and respond (Childnet)
- Cyberbullying: advice for headteachers and school staff (DfE)
- Help your child stay safe online (DfE, for parents)

10.2 National Organisations

- Action Fraud: www.actionfraud.police.uk
- CEOP: https://www.ceopeducation.co.uk/
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org

- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professionals Online Safety Helpline: https://saferinternet.org.uk/professionals-online-safety-helpline
  - Telephone helpline: 0344 381 4772
  - Email: helpline@saferinternet.org.uk

Appendix 1: Guided Home Learning and Live Online Teaching

Following the COVID-19 outbreak in 2020, GDST schools developed extensive experience of Guided Home Learning and live online teaching. These approaches continue to form part of the educational offer, supporting a range of provision including learning during periods of disruption, support for individual pupils, online tutoring and cross-school programmes such as ConnectEd. As technology and educational practice continue to evolve, the GDST will continue to develop and enhance these approaches where they support positive educational outcomes for pupils.

Some online learning may involve pupils being taught by staff from another GDST school; where this is the case, the schools will ensure that clear arrangements are in place for attendance, behaviour, pastoral support, safeguarding and communication.

The school is committed to ensuring that high standards of safeguarding, pastoral care and online safety are maintained across all forms of Guided Home Learning and live online teaching. Alongside the provisions in the Safeguarding and Child Protection Policy, Online Safety Policy, GDST Social Media Policy, Staff Code of Conduct and Acceptable Use Agreements for staff and pupils, the guidelines below must be followed.

Providing a safe system

- For the purposes of Guided Home Learning and Live Online teaching, the primary platforms used across the GDST network are:
    - Microsoft Teams
    - Google Classroom
    - Firefly

  The GDST has central oversight of and can monitor activity and communications through these platforms. The platforms are restricted to GDST users only and permissioned accordingly. Other platforms may be used at times for specific purposes. The online safety implications of any platform are carefully considered before use, and will be a key consideration in any decisions on configuration.
- Any activity involving non-GDST users (e.g. visiting speakers or pupils from other schools) will be risk assessed. Virtual visiting speakers are vetted and supervised in the same way as they would be if they were coming onto the school site to deliver their material.
- Some live online sessions are recorded for safeguarding purposes (as set out below). When a recording is made, access is restricted to participants and the IT Administrator. Access may be granted to others in the event of a complaint, formal investigation, or legal request (this would be carried out under the standard GDST policies). Further distribution is strictly prohibited. Recordings will be deleted after 12 months.
- Where online learning takes place between schools, including through ConnectEd, staff should be clear about safeguarding, attendance, behaviour and reporting arrangements, and should follow any programme-specific guidance regarding roles, responsibilities and communication channels.

Formats for home learning

There is a wide range of formats for guided home learning, including:

- Posting activities for pupils at regular intervals, with pupils posting responses
- Providing recorded material in the form of podcasts or video tutorials
- Directing pupils to web-based resources and activities they can engage with on or offline.
- Interactive/live teaching in real time

Teachers will select the most appropriate format depending on a number of factors, including the age of the pupils, size of the group, nature of the activity, and the degree of support required; and taking into account the need to provide a variety of learning experiences within a lesson, across the school day/week and through a scheme of work.

Live online teaching

Live online teaching is an important part of the educational offer for pupils of all ages and can support a range of provision, including remote learning during periods of disruption, online tutoring, and cross-school programmes such as ConnectEd. The educational purpose, delivery model and associated safeguards may vary according to context, and school will ensure that online provision is appropriate to the needs of pupils and the intended learning outcomes.

Interaction with a teacher and peers remains an important part of the learning process. Live sessions can provide valuable opportunities for discussion, feedback, collaboration and pastoral support, whilst helping pupils maintain important social connections.

Additional guidance relating to specific delivery models, including ConnectEd, is available in the relevant programme handbooks and operational guidance. Staff should ensure they are familiar with any requirements that apply to the particular online provision they are delivering.
In order to safeguard both pupils and staff, live online sessions must be conducted following the protocols set out below.

For staff:

- Only use school approved platforms; do not use social media in communicating with pupils
- Keep a record/log of live online lessons – date and time, attendance, what was covered, any incidents. Any serious incidents should be reported in the usual manner depending on the nature of the issue. For ConnectEd, refer to the dedicated staff handbook which sets out pastoral procedures for the specific partnership.
- Maintain professional conduct during live streaming – dress appropriately, consider your surroundings (background, other household members who may come into view etc.) and blur if necessary, and remember that your microphone may be on
- Maintain the same boundaries and insist on the same standard of behaviour as in a school setting. Make specific protocols clear at the outset, e.g. muting of microphones at appropriate times, use of supervised chat only, etc.
- The Head must be advised in advance of any 1:1 sessions. All 1:1 teaching sessions must be recorded on Microsoft Teams or Google Classroom. Support and pastoral 1:1 sessions should be recorded on Teams or Google Classroom unless the professional judgement of the member of staff is that this would be inappropriate, or the pupil is unhappy about a recording being made, in which case it is acceptable for detailed notes to be kept instead. Distribution of the recording beyond participants who have automatic access is strictly prohibited.
- Where teaching pupils from other GDST schools through programmes such as ConnectEd, understand and follow the agreed arrangements for attendance, behaviour, safeguarding and communication.

For pupils:

- Always log on through your GDST account and use your GDST email for school business

- GDST platforms may only be used for school business. Do not set up or engage in any activity which is not connected to school business and endorsed by your teachers
- Do not make recordings, take screenshots/screengrabs or photographs, or store or distribute footage of teachers or other pupils
- Be aware that some live online sessions may be recorded by the teacher
- Dress appropriately for online lessons
- Ensure that you have a safe and appropriate place to participate from. Blur your background if necessary
- Follow the school rules for conduct during online lessons as if you were in school
- Do not undermine in any way the technology used to offer video lessons
- Engage respectfully and positively with teachers and pupils from other schools when participating in online learning activities, including ConnectEd.
- Recognise that the expectations for conduct, participation, attendance, effort and academic integrity in online lessons are the same as those that apply in any face-to-face lesson.
- If you have concerns about online safety, or if you feel you are being bullied, talk to someone you trust
- There are also external reporting routes you can use:
    - Childline – for support
    - CEOP – to make a report about online abuse
    - UK Safer Internet Centre – to report and remove harmful online content

The role of parents:

- It is the responsibility of parents to ensure that pupils are monitored in their use of technology for Guided Home Learning as they would ordinarily do when their children are using technology at home.
- While students are working from home they are connected to their home broadband so their internet traffic doesn't go through the GDST firewall – parents will therefore need to ensure that age-appropriate filtering or safe search is enabled at home. Use of Chrome signed in with a GDST account gives some filtering and monitoring protection to the student, but this should not be relied upon as an internet safety solution at home.
- Communication during online learning is between student and teacher: parents should communicate with school/staff in the usual manner, via school email or telephone
- Parents with queries about Guided Home Learning should contact their child's class teacher or tutor. Concerns related to safeguarding, child protection or online safety should be referred to the DSL
- Incidents can also be reported to CEOP https://www.thinkuknow.co.uk/parents/Get-help/Reporting-an-incident/ or Report Harmful Content https://reportharmfulcontent.com/

Appendix 2: Use of Personal Devices and Mobile Phones

The school recognises 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.

1. Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: *Anti-Bullying*, *Behaviour and Discipline*, and *Safeguarding and Child Protection*.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times. The school accepts no responsibilities for the loss, theft, damage or breach of security of such items on school premises.
- In accordance with DfE guidance and GDST policy, GDST schools are mobile phone free for pupils up to Year 11. Arrangements for Sixth Form students reflect their increased independence and maturity, however, any access to mobile phones for Years 12 and 13 will remain clearly defined, limited in time and location, and grounded in the school's behaviour policy.
- The sending of abusive or inappropriate messages/content is forbidden by any member of the community; any breaches will be dealt according to the behaviour policy.
- All members of the 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 and Child Protection* policies.

2. Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that the 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 and Child Protection*, *Data Security* and *Acceptable Use Agreements*.
- Personal digital recording devices must not be used for taking, editing or transferring images or videos of pupils.

3. Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Pupils' personal smart devices and mobile phones are expected to be switched off and stored in the yondr pouch on arrival at school.
- If a pupil needs to contact his/her parents or carers they will be allowed to use their mobile phone or a school phone, as long as they have permission from their Head of Year or a member of SLT.
- Parents are advised to ONLY contact their child via the school office during school hours.
- Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's grade in that examination or all examinations being nullified.

- If a pupil breaches the school policy, their phone or device will be confiscated and will be held in a secure place
    - Searches for and of mobile phone or personal devices will only be carried out in accordance with the relevant government guidance.
    - Schools are not required to inform parents before a search takes place or to gain consent for a search for a prohibited item, or item which a member of staff reasonably suspects has been or is likely to be used to commit an offence or to cause personal injury or damage to the property of any person.
    - A search without consent will only be conducted by a member of staff of the same sex as the pupil being searched and authorised by the Head. There will also be a member of staff acting as a witness who will also, if possible, be of the same sex. A pupil's possessions will only be searched in the presence of the pupil and a witness.
    - Where the person conducting the search finds an electronic device that is prohibited by the school rules or that they reasonably suspect has been, or is likely to be, used to commit an offence or cause personal injury or damage to property, they may examine any data or files on the device where there is a good reason to do so. They may also delete data or files if they think there is a good reason to do so, unless they are going to give the device to the police.
    - If the member of staff conducting the search suspects they may find an indecent image of a child, they should never intentionally view the image, or copy, print, share, store or save such images. The member of staff should confiscate the device, avoid looking at it and refer the incident to the DSL.
    - If there is a suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.
    - The confiscation and searching of a phone or other digital device will normally be carried out in consultation with a senior member of staff.

4. 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 Agreement* and other associated policies, such as *Anti-Bullying* and *Safeguarding and Child Protection policies.*
- The school will ensure appropriate signage and information is provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL of any breaches of school policy.