NORTHAMPTON HIGH SCHOOL

GDST MODEL ONLINE SAFETY POLICY

This policy applies to the whole school, including the Early Years Foundation Stage

1. Policy Introduction and Aims

The internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. However, these modern technologies have created a landscape of challenges and dangers that is still 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
- Enable all staff to work safely and responsibly, to model positive behaviour online and to manage professional standards and practice when using technology
- 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 material; for example pornography, racist or radical and extremist views, and in some respects fake news
- **Contact:** being subjected to harmful online interaction with other users; for example children can be contacted by bullies or people who groom or seek to abuse them
- **Commercial exploitation:** for example young people can be unaware of hidden costs and advertising in apps, games and website
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying

2. Policy Scope

This policy applies to all staff including 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, including:

- The GDST *Information Security Policy*
- The GDST *Data Protection Policy*
- The school's *Safeguarding and Child Protection Policy*
- The GDST *Safeguarding Procedures* (which incorporates the staff *Code of Conduct*)
- *Acceptable Use Agreements* (AUAs) for staff and pupils (See end of this document)
- The GDST *Social Media Policy*
- The school's *Behaviour and Discipline Policy*
- The school's *Anti-Bullying Policy*
- Staff *Communication Policy*

3. Roles and Responsibilities

- Rebecca Kneen is the Designated Safeguarding Lead (DSL) responsible for online safety
- *All* members of the community have important roles and responsibilities to play with regard to online safety:

3.1 The Head:

- Has overall responsibility for online safety provision
- 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 *Acceptable Use Agreements*), information security and data protection
- 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
- Ensures that online safety practice is audited and evaluated regularly in order to identify strengths and areas for improvement.

3.2 The Designated Safeguarding Lead (DSL):

- Takes day to day responsibility for online safety
- Promotes an awareness of and commitment to online safety throughout the school community
- Acts as the named point of contact on all online safety issues, and liaises with other members of staff or other agencies, as appropriate
- Keeps the online safety component of the curriculum under review, in order to ensure that it remains up to date and relevant to pupils
- 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
- Monitors pupil internet usage, taking action where required
- Maintains the online safety incident log and record of actions taken, and reviews the log periodically to identify gaps and trends
- Reports regularly to the Head and SLT on the incident log, internet monitoring, current issues, developments in legislation etc.

3.3 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 school's 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 policy is applied and updated on a regular basis, and oversees the school's monitoring system
- Report any filtering breaches or other online safety issues to the DSL, Head, GDST and other bodies, as appropriate
- Ensure that any safeguarding concerns are reported to the DSL, in accordance with the school's safeguarding procedures.

3.4 All school staff:

- Read, adhere to and help promote the online safety policy, *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 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 reporting to the DSL
- Know when and how to escalate online safety issues
- Take personal responsibility for professional development in this area.

3.5 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 *Acceptable Use Agreements* (see end of this document)
- 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.

3.6 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
- 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.

3.7 External groups:

- Any external individual/organisation must sign an *Acceptable Use Agreement* prior to being given individual access to the school network.

4. Education and Engagement

4.1 Education and engagement with pupils

The school curriculum includes age-appropriate lessons and activities on online safety for all pupils, intended to raise awareness, build resilience and promote safe and responsible internet 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
- 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 shown how to validate information before accepting its accuracy
- Teaching pupils to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- 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 *Acceptable Use Agreement* in a way which suits their age and ability by:

- Discussing the 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 *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, 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:

- 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
- Drawing parents' attention to the school online safety policy and expectations in newsletters and on the website
- Requiring parents to read the pupil *Acceptable Use Agreement* and discuss its implications with their children.

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 appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material
- Ensure, through online safety education and the school AUAs, that pupils know that the school's expectations regarding safe and appropriate behaviour online apply whether the school's networks are used or not

6. Safer Use of Technology

6.1 Classroom Use

- The school 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
    - 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
- Supervision of pupils will be appropriate to their age and ability
- All school-owned devices should be used in accordance with the school's 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
- Staff and pupils should consider copyright law before using internet-derived materials (and where appropriate comply with licence terms and/or acknowledge the source of information).

6.2 Filtering and Monitoring

- All schools within the GDST are centrally provided with their data connections via a dedicated network. All incoming data are screened by an application that provides real-time filtering and protects both networks and users from internet threats. It prevents a wide range of unwelcome material and malware from being available in schools while at the same time allowing access to material of educational value. The policy determining filtering is managed centrally, with different levels being applied depending on age group
- The system logs all internet access on GDST devices, and these logs can be accessed by the DSL for monitoring purposes. Flagged terms will also trigger alerts which the DSL may investigate. Concerns identified will be managed according to the nature of the issue
- There is also a centrally managed process for scanning email messages between staff and students for inappropriate language and behaviour. If there is an issue the HR department at Trust Office will be alerted and the matter taken up with the school. Email traffic between pupils is not scanned as a matter of course, but if concerns about contacts between pupils are raised, then a record of messages may be retrieved
- All members of staff are however 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
- All users are informed that use of school systems is monitored and that all monitoring is in line with data protection, human rights and privacy legislation.

Dealing with Filtering breaches

The school has a clear procedure for reporting filtering breaches:

- If pupils discover unsuitable sites, they will be required to alert a member of staff immediately
- The member of staff will report the concern (including the URL of the site if possible) to the DSL
- The breach will be recorded and escalated as appropriate
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as Internet Watch Foundation (IWF), the Police or Child Exploitation and Online Protection (CEOP).

6.3 Managing Personal Data Online

Personal data will be collected, processed, stored and transferred in accordance with the *General Data Protection Regulations and the GDST's Privacy Notices*. Full information can be found in the school's *Data Protection Policy*.

7. Social Media

7.1 Expectations

- The term social media includes (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger
- All members of the school community are expected to engage in social media in a positive, safe and responsible manner, at all times

7.2 Staff Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites is discussed with all members of staff as part of staff induction and is revisited and communicated via regular staff training opportunities
- Safe and professional behaviour is outlined for all members of staff as part of the staff *Code of Conduct*, staff *Acceptable Use Agreement* and *Social Media Policy*

7.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of online safety education, 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. The school will not create accounts specifically for children under this age
- The school will control pupil 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 not permitted via the school Wifi
    - Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities
- 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. 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.

8.1 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
- Mobile phones and personal devices are not permitted to be used in specific areas within the school site such as changing rooms, toilets and swimming pools. No mobile devices are to be used in the EYFS areas of school.

- 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 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.

8.2 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*.
- Images of pupils (other than a member of staff's own children) must not be stored on personal devices. Any image taken on personal devices must be transferred to school or GDST systems as soon as reasonably possible and the personal copy permanently removed.
- Mobile devices must not be used in the nursery and EYFS areas of school

8.3 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
- Pupil's personal devices and mobile phones are expected to be kept silent and out of sight during the school day.
- If a pupil needs to contact his/her parents or carers they will be allowed to use a their mobile phone or a school phone, as long as they have permission from a member of school staff
- Parents are advised to contact their child via the school office during school hours
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
- 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, the 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[1],
    - Schools are not required to inform parents before a search takes place or to seek 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
    - 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 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.

[1] See Searching, screening and confiscation: Advice for headteachers, school staff and governing bodies DfE January 2018

8.4 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.

9. Responding to Online Safety Incidents and Concerns

- 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 (sexting), cyberbullying and illegal content
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns
- Incidents will be managed depending on their nature and severity, according to the relevant school policies
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes in policy or practice as required
- 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.
- Where there is suspicion that illegal activity has taken place, the school will contact the 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 Local Authority first, to ensure that potential investigations are not compromised.

9.1 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.

9.2 Misuse

- Complaints about IT 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.

10. 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 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

11. Useful links and sources of advice

11.1 Guidance and resources

- Teaching Online Safety in School (DfE)
- Education for a Connected World (UKCIS)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS)
- Indecent images of children: guidance for young people
- Cyberbullying: understand, prevent and respond (Childnet)
- Cyberbullying: advice for headteachers and school staff (DfE)

11.2 National Organisations

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.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
  - Net Aware: www.net-aware.org.uk
- 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
  - Telephone helpline: 0844 381 4772

Policy Reviewed: May 2022
Policy Reviewed by: Adele O'Doherty, Acting Head

Appendix 1: Guided Home Learning

Following the COVID-19 outbreak, GDST schools moved to Guided Home Learning for the majority of pupils during periods of national lockdown. In the future, Guided Home Learning will continue to be a managed part of the curriculum, either as a means of providing support for individual pupils in specific circumstances, or as part of a more flexible and diverse educational offer which the school and the GDST will continue to develop and enhance over time.

The school is committed to ensuring that online safety standards are maintained in the delivery of Guided Home Learning. Alongside the provisions in the *Safeguarding and Child Protection Policy* and *Online Safety Policy*, the 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, 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.

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, e.g. PurpleMash
- 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 this overall package for pupils of all ages, and can provide an exciting and enriching opportunity for collaboration between GDST schools. Interaction with a teacher is an important part of the learning process, and whilst online contact cannot replicate face to face contact, live sessions are particularly helpful as

they allow contemporaneous communication, with students able to respond to staff questions – and vice versa. Live contact is also an important part of pastoral support, and gives pupils the opportunity to interact with peers and maintain important social connections.

However, it should be remembered that live online teaching remains 'one tool in the box' and, for the reasons set out above, it should be balanced alongside learning opportunities in a range of other formats.

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
- 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.

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
- 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 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. Information on setting this up can be found at: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/parental-controls-offered-your-home-internet-provider and here: https://www.internetmatters.org/parental-controls/
- 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/

Key Stage 1: Acceptable Use Agreement

This is how I keep **SAFE online**:	✔
1. I only use the devices I'm **ALLOWED** to	
2. I **CHECK** before I use new sites, games or apps	
3. I **ASK** for help if I'm stuck	
4. I **THINK** before I click	
5. I **KNOW** people online aren't always who they say	
6. I don't keep **SECRETS** just because someone asks me to	
7. I don't change **CLOTHES** in front of a camera or webcam	
8. I am **RESPONSIBLE** so never share private information such as my address, phone number or passwords	
9. I will only send **KIND** and polite messages	
10. I **TELL** a trusted adult if I'm worried, scared or just not sure	

My trusted adults are _____ at school

and _____ at home.

My name is _____

Key Stage 2: Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others.

- ***I am an online digital learner*** – I use the internet and email for schoolwork, homework and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.
- ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. I don't leave my computer unattended if I am logged on.
- ***I am careful online*** – I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.
- ***I am private online*** – Private information is information that could be used to identify me or my friends and family, like addresses, phone numbers, photos or who my friends are. I do not give out private information unless a trusted adult says it's okay.
- ***I keep my body to myself online*** – I never change what I wear in front of a camera or webcam and remember that my body is mine and mine only. I don't send any photos without checking with a trusted adult.
- ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.
- ***I am a rule-follower online*** – I know that some websites and social networks have age restrictions and I respect this. I only visit sites, games and apps that my trusted adults have agreed to.
- ***I am considerate online*** – I do not join in with bullying or sharing inappropriate material. I keep others safe by talking to my trusted adults if a friend or person I

know is being bullied or harassed or is worried or upset by things they read, watch or hear.

- ***I am respectful online*** – I do not post, make or share unkind, hurtful or rude messages/comments/photos and tell my trusted adults if I see these.
- ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
- ***I am responsible online*** – I don't try to buy things online even if I really, really want them unless my trusted adult helps me.
- ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.
- ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
- ***I am smart online*** – I understand that unless I have met people in real life, I can't be sure who someone is online, so if I want to meet someone for the first time, I must always bring a trusted adult with me.
- ***I am a creative digital learner online*** – I only edit or delete my own digital work and only use other people's with their permission.
- ***I am a researcher online*** – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, and know I should verify information I find online.

My trusted adults are:_____

If I feel I can't talk to them, I know I can call Childline on 0800 1111 or click CEOP.

I have read and understood this agreement.

Signed: _____ Date: _____

Key Stage 3-5: Acceptable Use Agreement

I will be a **responsible user and stay safe** when using the internet and other digital technology.

Following these rules will help to keep everyone safe and be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies and online services.

Responsible User

1. I will ensure that my online activity or use of mobile technology, in school or outside school, **will not cause my school, the staff, students or others distress**, or bring the school into disrepute.
2. I understand that whilst in school **GDST provided Wi-Fi is filtered and device use is monitored**. I also understand that all school-owned devices used outside of school may be subject to filtering and monitoring, and should be used as if I am in school.
3. I will only use my **personal devices** (mobile phones, USB devices etc.) in school if I have been given permission to do so.
4. I will only use the **school's internet** and any device I may be using in school for appropriate school activities and learning, unless I have permission to engage in recreational activities, e.g. in a lunchtime club or after school.
5. I will only use my **school email and account details** to contact people as part of learning activities.
6. I will keep my **logins, IDs and passwords** secret and change my password regularly. If I think someone knows one of my passwords, I will change it. I will not leave my computer unattended if I am logged on and will only log in with my username and password.
7. I will not knowingly **bring files into school or download files** that can harm the school network or be used to bypass school security, such as VPN programmes.
8. I will be careful when **opening files and attachments**, checking for viruses etc. If I am unsure I will never open a file, hyperlink or any other attachment. If I am suspicious about a file or attachment, I will let a teacher or member of the ICT support team know.
9. I will only **edit or delete** my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
10. I understand that websites, blogs, videos and other **online information can be biased** and misleading, so I need to check sources to see if they are trustworthy.
11. When using the internet, I will not download **copyright-protected material** (text, images, music, video etc.). I will always make sure I acknowledge the sources of information I find on the internet if I use it for my work or pass it on to friends.

Stay Safe

12. I understand that **cyberbullying** is unacceptable, and will not use technology to bully, impersonate, harass, threaten, make fun of, exclude or upset anyone, at school or outside school.

13. I will not browse, download, upload, distribute, post, retweet or forward material that could be considered **discriminatory, offensive, harmful, illegal or of a sexual nature**. If I accidentally come across any such material I will report it immediately to my teacher.
14. The messages I send, or information I upload, will always **be polite and sensible**. I understand that all messages I send reflect on me and the school.
15. I will not share my or others' **personal information** that can be used to identify me, my family, my friends or my school on any online space, unless a trusted adult has given permission or reviewed the site.
16. If **live streaming** I always tell a trusted adult about it and check my privacy settings so I am in control of who can see my stream.
17. I will never arrange to **meet someone face to face** if I have only ever previously met them on the internet or by e-mail or in a chat room, unless I take a trusted adult with me.
18. I will **respect my body and other people's**. That means using positive words about myself and others. It also means not revealing my or anyone else's body on camera or sharing /posting inappropriate photos.
19. I am aware that some websites, apps, games, online shopping, file sharing and social networks have **age restrictions** and I will respect these. I will ensure sites are secure if exchanging personal or financial information.
20. I understand that many apps have **geolocation** settings (identifying my location or where I made a post or took a photo). I will make sure that I know how to turn geolocation on and off, and not tell the world where I am at all times or make it too easy to find out where I live or go to school.
21. If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, extremist/hateful content, **I will not respond and talk to a trusted adult**.
22. I know that I **can always say no** online and end a chat or block a friend; if I do, it's best to talk to someone about it as well.
23. I **know who my trusted adults are** at school, home and elsewhere, but if I feel I can't talk to them, I know I can call Childline on 0800 1111 or click CEOP.

The trusted adults I can talk to if I have concerns about e-safety are:

_____

I have read and understand these rules and agree to them.

Signed: _____ Date:_____