REDDIFORD SCHOOL

INCLUDING EYFS

E-SAFETY POLICY

To be used in conjunction with:
Safeguarding Policy
Whistleblowing Policy
Low Level Concerns Policy
Photographic Images of Children Policy and Guidelines
Behaviour and Anti Bullying policies
Staff Disciplinary & Capability Procedures
Data Protection Policy
PSHE Policy
RSHE Policy
Staff Code of Practice and Expectations
Parent Code of Practice
Pupil Code of Practice
Data Protection Act 2018
The General Data Protection Regulation
Computer Misuse Act 1990
Human Rights Act 1998
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
Education Act 2011
Freedom of Information Act 2000
The Education and Inspections Act 2006
Keeping Children Safe in Education 2024
Searching, screening and confiscation: DfE advice for schools (January 2018)
Obscene Publications Act 2019
www.gov.uk/guidance/safeguarding-and-remote-education 2022
Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS, 2020)
meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges 2023
saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring 2023

Updated September 2024

1. Introduction and Aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of Reddiford School.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding. This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding, which includes protecting children from maltreatment, whether that is within or outside the home, including online.
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Staff Disciplinary & Capability Procedures, Behaviour and Anti-bullying policies.

2. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, apps, email, online teaching and learning (e.g. Satchel One), meetings (Teams) and technical support (LogMeIn 123) platforms and any device, system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

3. Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see 3.2 Sanctions below).
Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright.
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate. (See Appendix 4 in SCOPE for staff advice on procedures to follow if sharing nude and semi-nude images incident occurs).
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its pupils, or other members of the school community.
- Connecting any device to the school's ICT network without approval from authorised personnel.
- Installing or configuring any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to ICT facilities.
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the school.
- Using websites or mechanisms to bypass the school's filtering mechanisms.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

3.1 Exceptions from Unacceptable Use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion, approval must be sought in advance.

3.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on staff disciplinary and pupil behaviour. The Behaviour and Anti Bullying policies can be found on the school website (under policies), and Staff Disciplinary & Capability Procedures can be obtained from the staff portal.

4. Staff (including Governors, Volunteers and Visitors)

4.1 Access to school ICT facilities and materials

The school's network manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, laptops, school mobile phones and other devices
- Access permissions for certain programs or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should speak to the Headteacher.

4.1.1 Use of Phones and Email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their work email or personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account. The only exceptions to this are:

- The Bursar
- The Assistant Bursar
- The Registrar
- Upper and Lower School Departmental Secretaries

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 and Freedom of Information Act 2000 in the same way as paper documents.

Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the Data Protection Officer (Bursar) immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. School phones must not be used for personal matters. When offsite school mobile phones must be used to communicate with parents and the number should be blocked.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out above.

4.2 Personal Use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours/non-break time/contracted hours for support staff.
- Does not constitute 'unacceptable use', as defined above.
- Takes place when no pupils are present.
- Does not interfere with their jobs or prevent other staff or pupils from using the facilities for work or educational purposes.

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section below). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's personal device policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix in SCOPE) and use of email (see section above) to protect themselves online and avoid compromising their professional integrity.

4.2.1 Personal Social Media Accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for social media accounts (see SCOPE appendix 3).

4.3 Remote Access

Staff are provided with remote access to emails and selected externally-hosted resources. Staff accessing email facilities and resources remotely must abide by the same rules as those accessing the facilities and resources on-site. Staff must be particularly vigilant when using ICT facilities outside of the school and take any precautions required by the ICT Manager to avoid importing viruses or compromising system security.

The ICT Manager, Senior Management Team and Assistant Bursar have remote access via RDP (over VPN). This is managed under the supervision of the Bursar/Head Teacher.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

The school's data protection policy can be requested from the school.

4.4 Monitoring of School Network and Use of ICT Facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff and the DSL for safeguarding purposes may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

5. Pupils

Pupils are educated in PSHE and ICT lessons on how to safely use the internet, ensuring they are aware of the potential dangers of malicious use of technology, in addition to the issues surrounding cyber-bullying, teasing and threatening behaviour. The sharing of information, such as photographs and videos, is also discussed, with emphasis on accessing age-appropriate content.

5.1 Access to ICT facilities

- Computers, laptops, tablets and equipment in the school's classrooms and Learning Hub are available to pupils only under the supervision of staff.
- Specialist ICT equipment, such as that used for music or science must only be used under the supervision of staff.

5.2 Searching Electronic Devices

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

Reddiford staff would always inform parents if they suspected a pupil's mobile device contained unsuitable material which contravened school rules. If the material is thought to be illegal, staff would seek permission from the pupil or parent to view the material on their device.

However, there is no legal requirement for the school to seek the consent of pupils or parents before a search, when there are reasonable grounds to suspect a pupil is in possession of a prohibited item.

In line with advice from the DfE, parents will be made aware that any items deemed to be illegal can be passed onto Social Services and the Police. In such cases, advice will be sought from MASH (Multi Agency Safeguarding Hub) and/or CEOP (Child Exploitation and Online Protection Command) due to the age and understanding of Reddiford pupils (see Safeguarding Policy).

5.3 Unacceptable Use of ICT and the Internet Outside of School

The school will sanction pupils, in line with the Behaviour and Anti-Bullying policies, if a pupil engages in any of the following **at any time** (even if they are not on school premises). Additionally, the school Safeguarding policy aims to protect children from maltreatment, whether that is within or outside the home, including unacceptable online activity:

- Using ICT or the internet to breach intellectual property rights or copyright.
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination and abuse, neglect or exploitation of others.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, other pupils, or other members of the school community.
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to ICT facilities or materials.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.

6. Parents

6.1 Access to ICT Facilities and Materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a PTA volunteer) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

6.2 Communicating with or about the School Online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through email. We ask parents to sign the agreement in appendix 3.

7. Data Security

The school takes all reasonable steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee absolute security. Staff, pupils, parents and others who use the school's ICT facilities should implement safe computing practices at all times.

7.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts.

If staff suspect their password has been compromised, they must inform the ICT Manager immediately.

The ICT Manager, authorised by the Headteacher, is responsible for setting permissions for staff accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action.

Parents or volunteers who disclose account or password information may have their access rights revoked.

7.2 Software Updates, Firewalls, Anti-Virus Software, Filtering and Monitoring

ICT devices eligible for software and security updates will be updated regularly or configured to perform automatic updates. This includes, but is not limited to, endpoint protection definitions, operating system security updates and networking hardware firmware.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities. Any personal devices using the school's network must all be configured in this way.

The school uses the WebScreen 3.0 filtering system. This solution was carefully designed for the needs of the education sector and is continually maintained and updated by the London Grid for Learning (LGfL) Trust. This system also facilitates report generation, allowing us to capture blocked URLs, when they were visited and the workstation that was used.

We use a managed Cisco ASA 5515-X firewall to restrict external access to the school network, thus preventing student data becoming compromised through unauthorised server access. The school wireless network requires active directory user account authentication and has been configured to allow staff access only.
We also use Smoothwall to filter, monitor and report all inappropriate searches and content on school ICT equipment.

7.3 Data Protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy. The data protection policy can be requested from the school.

Access to personal data is restricted to the administration staff and SMT. Access to removable media (USB flash drives, writeable discs) is blocked for students and regulated for staff.

Data is backed-up regularly to multiple sites. All off-site backups are stored using 256-bit AES encryption.

7.4 Access to Facilities and Materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the ICT Manager.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the ICT Manager immediately.

Users should always log out of systems when they have finished working. Systems and equipment should be locked when it is not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

7.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption. Two factor authentication is required for accessing Share Point/One Drive (cloud storage). School staff may only use personal devices (including mobile phones, computers and tablets) to access school data, work remotely, or take personal data (such as pupil information or parent contact details) out of school if they have been specifically authorised to do so by the Headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT Manager.

8. Internet Access and Online Safety

It is essential that children are safeguarded from potentially harmful and inappropriate online material. All staff are aware that abuse can take place wholly online, and they understand that the use of technology is a significant component of many safeguarding issues e.g. in incidents of cyber-bullying, child sexual exploitation, radicalisation, and sexual predation.
The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, misandry, 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 financial scams.

We 'consider a whole-school approach to on-line safety', doing all that we can to minimise the risk of exposure to harmful online material through the School's IT system. This includes appropriate filtering and monitoring systems which are reviewed at least annually and meet the DfE's filtering and monitoring standards.

The school Internet connection is filtered by LGfL (Atomwide/AdEPT Education). All users are responsible for reporting inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) to the ICT Manager. We also use Smoothwall (and Impero) to filter, monitor and report inappropriate searches and content. Smoothwall contact the ICT Manager, DSL and SMT via email with alerts as and when required.

The school's wireless network is secured to prevent unauthorised access to the school Internet connection.

The school ensures that the appropriate filters and monitoring systems which are in place to safeguard children, do not cause an unreasonable level of blocking which can impact teaching and learning and administrative tasks.

Additionally, there are ICT Acceptable Use Agreements and a clear use on mobile and smart technology guidance for all stakeholders (see SCOPE). The content of the Acceptable Use

Agreements is highlighted to all parents and pupils at least annually. We also consider carefully how to manage 3G, 4G and 5G accessibility on the school's premises.

Online safety training for staff and pupils is an integral part of our overarching approach to safeguarding. It is encompassed within the annual safeguarding training that all staff complete; all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring, including how to escalate concerns once identified.

The Designated Safeguarding Lead (DSL) has lead responsibility for online safety, staff training and for understanding and annually reviewing the filtering and monitoring systems and processes in place. The DSL will liaise with the ICT Manager when alerts are produced by the filtering system and follow up as appropriate with the Head teacher and SMT.

The DSL is supported by the following colleagues who work together to ensure that the DfE's filtering and monitoring standards are met:

- The Headteacher (has level 3 training) liaises with the Governors to create a whole-school approach to online safety education and ensures that they are kept informed of all updates and requirements in this area;

- The ICT Manager is responsible for ensuring and maintaining a safe technical infrastructure at the school, the security of all hardware systems, virus protection is updated regularly, that use of the school Wi-Fi is monitored on all IT devices in School, informing the DSL when monitoring alerts are produced by the filtering system, and keeping abreast of the rapid succession of technical developments;

- The Deputy Head Academic (Deputy DSL) working with the PSHE and ICT Coordinators is responsible for ensuring the curriculum educates pupils on this topic, and liaising with the Headteacher, DSL and ICT Coordinator to update ICT Acceptable Use Agreements for all stakeholders;

- The ICT Coordinator is responsible for training teaching staff in the use of technology, including Impero software for actively monitoring pupil use of learning devices in lessons, updating the Pupil Acceptable Use Agreements (with the DSL/DDSL) and ensuring that every student has read and agreed to keep to the terms of the AUA;

- The Safeguarding Governor is responsible for overseeing online safety, including oversight of the annual review of filtering and monitoring;

- Head of Upper School (has level 3 training) is responsible for overseeing the education of Prep pupils and parents on topics related to online safety; works with the Deputy Head Pastoral (DSL) on Impero alerts relating to Prep department pupils and creating a whole-school approach to online safety education;

- Head of Lower School (has level 3 training) is responsible for overseeing the education of Early Years and Pre Prep pupils and parents on topics related to online safety; works with the Deputy Head Pastoral (DSL) on Impero alerts relating to Early Years and Pre

Prep department pupils and creating a whole-school approach to online safety education.

We keep our parents up to date regarding online safety by providing reputable resources and information and discussing the matter at relevant parent information evenings. For information regarding Remote Teaching and Learning please see Appendix 5.

8.1 Pupils

Pupils are not permitted to bring personal devices to school. Pupils who walk to school by themselves may bring a mobile phone to school but this must be switched off and left with the Deputy Head during the day. Internet enabled wearable devices such as smartwatches are not allowed to be worn at school. Pupils are not allowed to access the school's Wi-Fi, VPNs or mobile hotspots on their personal devices when on school premises. They are always supervised by staff, when using school internet-based resources in lessons.

8.2 Parents, Visitors and Visiting Staff

Parents, visitors and visiting staff to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the headteacher.

The Headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA).
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan).
- Visiting staff i.e. for clubs require limited access to the school network.

Staff must not give logins, passwords and Wi-Fi connection credentials to anyone who is not authorised to have it. Doing so could result in disciplinary action.

9. Monitoring and Review

The Headteacher, Designated Safeguarding Lead (Deputy Head Pastoral) and ICT Manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed annually.

The Headteacher is responsible for approving this policy.

APPENDIX 1

REDDIFORD SCHOOL
EYFS & PRE PREP PUPILS
ICT ACCEPTABLE USE AGREEMENT

Updated September 2024

REDDIFORD SCHOOL EYFS & PRE PREP PUPILS

ICT ACCEPTABLE USE AGREEMENT

This ICT Acceptable Use Agreement will help me to:

- stay safe while using the internet and other digital technologies at school and home;
- be fair to others when I use the internet and digital devices.

1. I only **USE** digital devices or apps, sites or games if a trusted adult says I can. ☐
2. I **ASK** for help if I'm stuck, make a mistake or not sure. ☐
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused. ☐
4. If I see something I do not like on the screen and **FEEL UPSET**, I talk to a trusted adult. ☐
5. I look out for my **FRIENDS** and tell someone if they are worried or need help. ☐
6. I **KNOW** people online aren't always who they say they are. ☐
7. Anything I do online can be shared and might stay online **FOREVER.** ☐
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to. ☐
9. I don't change **CLOTHES** or show what's under my clothes in front of a camera. ☐
10. I always speak to a trusted adult before **SHARING** personal information. ☐
11. I am **KIND** and polite and will never use a digital device to be hurtful to anyone. ☐

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult at school or home.

Name: _____ **Class:** _____

Signed: _____ **Date:** _____

Updated September 2024

APPENDIX 2

REDDIFORD SCHOOL
PREP PUPILS
ICT ACCEPTABLE USE AGREEMENT

Updated September 2024

REDDIFORD SCHOOL PREP PUPILS' ICT ACCEPTABLE USE AGREEMENT

This ICT Acceptable Use Agreement is intended to ensure:

- that I will be a responsible user and stay safe while using the internet and other digital technologies for educational, personal and recreational use (both in and out of school);
- that I will always be fair to others when I use the internet and digital equipment;
- and that I will stay safe online by always remembering the following points.

1. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords! I will only use the school WiFi network when in school and never try to use a VPN or personal hotspot.

2. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too.

3. ***I communicate and collaborate online*** – at home with people I already know and have met in real life or that a trusted adult knows about with parental guidance. I do not access email, social media websites or games whilst in school.

4. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.

5. ***I check with an adult before I meet an online friend*** face to face for the first time, and I never go alone.

6. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

7. ***I don't take photos or videos of people without them knowing or agreeing to it*** – and I never film people when they are upset or angry.

8. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

9. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.

10. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

11. ***I am private online*** – I do not give out private information when I am online. This could include my name, address, email, phone number, age, gender, school details, financial details, location or anything else that could identify me or my family and friends.

12. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).

13. ***I learn online*** – I use the school's online learning platforms (e.g. Satchel One, Language Angels, TTRS), internet and devices for schoolwork, homework and other activities to learn and have fun. I understand that the school's online learning platforms, internet and devices are monitored.

14. ***I learn even when I can't go to school*** – I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom. If I get asked or told to do anything that I would find strange in school, I will tell a trusted adult.

15. ***I ask permission*** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.

16. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.

17. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.

18. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets or worries me on an app, site or game – it often helps. If I get upset, I talk about it.

19. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.

20. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. 13+ games, apps and films aren't good for me, so I don't use them – they may be scary, violent or unsuitable. I follow the rules, age restrictions, block bullies and report bad behaviour.

21. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.

22. ***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.

23. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.

24. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult at school or home.

Name: _____ **Class:** _____

Signed: _____ **Date:** _____

Updated September 2024

APPENDIX 3

REDDIFORD SCHOOL
PARENTS
ICT ACCEPTABLE USE AGREEMENT

Updated September 2024

REDDIFORD SCHOOL PARENTS ICT ACCEPTABLE USE AGREEMENT

We ask all children and adults involved in the life of Reddiford School to sign an ICT Acceptable Use Agreement, which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Your child has also signed an ICT Acceptable Use Agreement which is attached. These rules have been written to help keep everyone safe and happy when they are online or using technology.

School systems and users are protected and monitored by security and filtering services to provide reasonably safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe.

We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

If you have any questions about the following agreement or our approach to online safety, please speak to your child's class teacher.

1. I understand that Reddiford School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering.
3. School network protections will be superior to most home filtering. However, please note that accessing the internet always involves an element of risk and the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies. Schools are asked not to overblock or provide an experience which is so locked down as to block educational content or not train pupils for life in an online world.
4. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school is subject to filtering and monitoring. These should be used in the same manner as when in school.
5. I understand and will help my child to use any devices at home in the same manner as when in school, including during any remote learning periods.

6. I will support my child to follow the school's policy regarding bringing mobile phones to school and not accessing the school's Wi-Fi, VPNs or mobile hotspots on their personal device. (Only pupils who walk to school by themselves are permitted to bring a mobile phone to school which must be switched off and left with the Deputy Head during the day).
7. I understand that my child might be contacted online on Satchel One by their form or subject teachers, or head of department only about their learning. If they are contacted by someone else or staff ask them to use a different app to chat, they will tell the Headteacher, Deputy Head Pastoral (DSL) or Deputy Head Academic (Deputy DSL).
8. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
9. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will monitor my child's use of digital devices at home, ensuring safe use of appropriate websites and adhere to age restrictions applicable to social media platforms, apps, films and gaming.
10. I will support and follow the school's Photographic Images of Children Policy and Guidelines which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
11. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety. Understanding human behaviour is more helpful than knowing how a particular app, site or game works.
12. I understand that my child needs a safe and appropriate place to do home learning, whether for homework or during times of school closure. When on any video calls with school, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
13. If my child has online tuition, I will refer undertake necessary checks where I have arranged this privately, ensuring they are registered/safe and reliable, and for any tuition to remain in the room where possible, ensuring my child knows that tutors should not arrange new sessions or online chats directly with them.
14. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet and to various devices, operating systems, consoles, apps and games. There are also child-safe search engines e.g.

swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content. Find out more at parentsafe.lgfl.net.

15. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
16. I understand and support the commitments made by my child in the ICT Acceptable Use Agreement which s/he has signed, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
17. I can find out more about online safety at Reddiford School by reading the full E Safety Policy (available on the school website) and can talk to my child's form tutor, if I have any concerns about my child's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

----------✂----------

REDDIFORD SCHOOL PARENTS ICT ACCEPTABLE USE AGREEMENT

As a parent / guardian I understand these rules and procedures are to safeguard my child's use of ICT, both in and outside of school. I therefore agree to support these statements and the school's efforts to safeguard its pupils.

Name of parent/guardian: _____ Signed: _____

Name of child: _____ Form: _____ Date: _____

APPENDIX 4

REDDIFORD SCHOOL STAFF, GOVERNORS, VOLUNTEERS & VISITORS ICT ACCEPTABLE USE AGREEMENT

Updated September 2024

Staff, Governors, Volunteers & Visitors ICT Acceptable Use Agreement

New technologies have become integral to the lives of children in today's society, both within and outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and enhance awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- That staff will be responsible users and stay safe while using the internet and other communications technologies for educational, administrative, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.
- That staff safeguard and promote the welfare of pupils at the school.
- That staff have a clear understanding of how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

All staff, governors, volunteers and visitors with access to the ICT network are required to read and sign it.

This Acceptable Use Agreement (AUA) is reviewed annually, and staff, governors, volunteers and visitors are asked to sign it when starting at the school and whenever changes are made. All staff (including support staff), governors and volunteers have particular legal / professional obligations, and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the E Safety Policy, Safeguarding Policy and SCOPE.

If you have any questions about this AUA or the school's approach to online safety, please speak to a member of the Senior Management.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of ICT for increasing effectiveness and efficiency in administrative tasks and enhancing teaching and learning. I will ensure that pupils receive opportunities to gain from the use of digital technologies and where possible, educate them in the safe use of ICT by embedding e-safety in my daily work practice.

For my professional and personal safety:

- I have read and understood Reddiford School's full E Safety policy and agree to uphold the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils. I will report any breaches or suspicions (by adults or children) without delay as outlined in SCOPE and the Safeguarding and E Safety policies.
- I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, ICT systems, internet, email and other digital communications and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/ captured/viewed by the relevant authorised staff members as it is vital that network security is not compromised through misuse.
- I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE 2023, now led by the DSL. If I discover pupils may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay.
- I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area.
- I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult).
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, tablets, website, online teaching platforms, Zoom, Teams, email, iPads, mobile phones, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will follow the guidance in the Safeguarding Policy, E Safety Policy and SCOPE to immediately report any illegal, inappropriate or harmful material or incident, (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media) I become aware of, to a member of the Senior Management.
- I will follow best-practice pedagogy for online-safety education, avoiding scaring and other unhelpful prevention methods. See onlinesafetyprinciples.lgfl.net for further guidance.
- I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

Ensuring pupil safety:

- When using electronic devices with pupils (e.g. tablets, computers, laptops), I will remain in the room at all times and ensure that the devices are used appropriately by pupils.
- Whilst access to unsuitable internet content is minimised by filtering software, this can never be completely eliminated. I will ensure that pupils do not access or search for inappropriate content by applying suitable security measures e.g. using the Impero software program to monitor pupils use of ICT.
- I will remind pupils not to divulge personal information online (including through e-mail).
- I understand that it is the responsibility of all staff to ensure that pupils do not have access to confidential data, and I must therefore be vigilant in my security measures – for instance, locking my computer when leaving the room for a short period of time.
- For reasons of child protection, I will not store any pupil data, video or photographs online.
- I will not store photographs or videos of pupils on any personal devices e.g. camera, mobile phone, tablet (see SCOPE and Safeguarding Policy).
- I understand that all instances of staff attempting to access inappropriate material or using ICT facilities irresponsibly, will be treated as a serious matter. Disciplinary action and police involvement may result.
- I will not upload, download or access any materials which are inappropriate, or may cause harm or distress to others, or are illegal (child sexual abuse images, racist material, adult pornography covered by the Obscene Publications Act 2019). I will not use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- If I suspect that illegal content has been accessed on a computer, I will power down and secure the workstation. I will not attempt to check whether the content is illegal by accessing it and contact a member of Senior Management immediately.
- I will inform a member of Senior Management immediately if I suspect there has been an incident involving cyberbullying or radicalisation.
- I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom.
- I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including online bullying, sexual violence and harassment – know that 'it could happen here'!
- I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.
- I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the PSHE and ICT curriculum, both outside the classroom and within the curriculum, supporting staff, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

- When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites, including finding out what appropriate filtering and monitoring systems are in place and how they keep children safe.
- I will prepare and check all online sources and classroom resources before using for accuracy and appropriateness. I will flag any concerns about over blocking to the ICT Manager and DSL to inform regular checks and annual review of these systems.
- I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.
- During any periods of remote learning, I will not behave any differently towards pupils compared to when I am in school and will follow the same safeguarding principles as outlined in the Safeguarding Policy, E Safety Policy and SCOPE.

I will be professional in my communications and actions when using school ICT systems and personal devices:

- I will only use the internet or access emails for personal reasons on my own digital device during break / lunch times or outside lesson times.
- I will not use personal email addresses to correspond on school matters.
- I will not use the school's name in the domain for personal email accounts.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's Photographic Images of Children Policy and Guidelines on the use of digital or video images. I will not use my personal devices to record these images unless permission has been granted by the Headteacher. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute.
- I will only use Zoom/Teams on a school device for school matters and will always sign in with the email address that matches the following domain '@reddiford.org.uk'. I will not use my school email address to create a personal account on Zoom/Teams.
- I will use caution when posting information online including on social networking sites and blogs. Staff posting material on social media sites which could be considered inappropriate, render themselves vulnerable to allegations of misconduct and disciplinary action (see SCOPE).
- I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's E Safety Policy and SCOPE. I will report any breach of this by others or attempts by pupils to do the same to the Headteacher.

- Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full E Safety policy and SCOPE. If I am ever unsure, I will ask the Senior Management.
- I understand that staff must not be 'friends' with, or communicate with, pupils and parents on 'Facebook', 'X-Twitter', 'Myspace' 'Snap Chat', 'Instagram', 'WhatsApp' or any other social networking website. Any staff contravening this rule, leave themselves open to disciplinary action and police investigation (see SCOPE and Safeguarding Policy).
- I will only communicate with parents or external organisations pursuant to my job role using official school mobile phones, email accounts and systems. I will ensure that nothing of a libellous or defamatory nature is included, and that all such communication will be professional in tone and manner.
- If the data on any device is breached, I will report it to the Data Protection Officer immediately (see Data Protection Policy).

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will consult with the ICT Manager before using any type of removable media devices as these can carry viruses or other malicious software. Permission to use removable media devices must be approved by the Headteacher.
- The ICT Manager / Headteacher has the right to confiscate any such media if they believe the use of such may compromise network security.
- I understand that ICT devices not purchased by the school should not be connected to the school's ICT network, except with prior approval from the Headteacher in exceptional circumstances.
- If permitted to use my personal external devices (e.g. laptops / mobile phones / tablets / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or attachments in emails, unless the source is known and trusted. If I have any concerns about the legitimacy of an email, I will consult the ICT Manager for guidance.
- Whilst data stored on the network is backed up regularly, I understand the importance of regularly backing up my work including data on removable storage devices.
- I will not install or attempt to install programs of any type on a device, or store programs on a computer, nor will I try to alter computer settings, unless permission is gained from the Headteacher.
- I understand that software installed on school owned ICT devices must be appropriately licensed. Budget holders have a responsibility to ensure that software purchased is licensed appropriately. Software installations on networked devices should be approved by the ICT Manager.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will not remove any confidential or sensitive material from the school site at any time, whether in electronic or paper form, without the approval of the Headteacher.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the information Data Protection Policy. Where digital personal data is transferred outside the secure school network, it must be encrypted and password protected. Paper based protected and restricted data must be held in lockable storage.
- I understand that the Data Protection Policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- It is my responsibility to understand and comply with current copyright legislation.

I understand that I am responsible for my actions in and out of school:

- I agree to adhere to all provisions of the school's cybersecurity procedures, SCOPE, Data Protection, E Safety and Safeguarding Policies at all times, whether or not I am on site or using a school device, platform or network.
- I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
- I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.
- I understand and support the commitments made by pupils, parents and fellow staff, governors and volunteers in their Acceptable Use Agreements and will report any infringements in line with school procedures.
- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement and school policies, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police and social services and termination of my relationship with the school.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

----------✂----------

I have read through and understand the "**Acceptable Use Agreement**" regarding staff, governors, volunteers & visitors use of ICT and agree to the above expectations. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent E Safety and Safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

NB. PLEASE COMPLETE AND RETURN THIS PAGE ONLY, RETAINING THE E SAFETY POLICY FOR YOUR OWN RECORDS.

Name: _____ Signature:_____

Date: _____ To be kept on staff member's records.

APPENDIX 5

REMOTE TEACHING & LEARNING

Updated September 2024

REMOTE TEACHING & LEARNING

Reddiford School is committed to providing a safe environment for online learning. This commitment remains the same in circumstances where teaching and learning are provided to pupils remotely (for example, due to enforced school closure or whilst staff are self-isolating for Covid reasons). During the period of Guided Home Learning our expectations of staff and pupils also remain the same, and the principles and practices of the school's Safeguarding Policy, E Safety Policy, Staff Code of Practice and Expectations and Acceptable Use Agreements for staff and pupils will continue to apply, both to existing and any new online and distance learning arrangements introduced. Staff and pupils must review these policies and ensure that they adhere to them at all times.

In order to ensure the safety and welfare of children during a period that pupils are engaging in guided home learning, the school will follow the DfE remote learning guidance:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1136309/Providing_remote_education_non-statutory_guidance_for_schools.pdf

The following guidelines will also apply:

Providing a safe system

- Where the school remains open, the school will continue to ensure that appropriate filters and monitoring systems are in place to protect children when they are online on the school's ICT systems or recommended resources.
- If the school is required to close, the primary platform used for the purposes of guided home learning, is Satchel One.

The school has central oversight of and can monitor all activity and communications through this platform. The Satchel One platform is restricted to Reddiford School users only and permissioned accordingly. Other platforms may be used at times for specific purposes e.g. Microsoft Teams for staff meetings or teaching whole classes whilst children are in school if a member of staff is shielding or required to isolate at home. Live online lessons delivered to children whilst in school or at home will not be recorded.

The online safety implications of any platform are carefully considered before use.

- The ICT Manager is responsible for maintaining a safe and operational online environment.
- The school's Designated Safeguarding Lead (DSL) has day to day responsibility for online safety and will maintain an active oversight of the management of guided home learning from a safeguarding perspective. Procedures will be kept under review and action will be taken swiftly if concerns about the use of technologies arise.

- The school will keep in regular contact with parents, updating them as appropriate with information on how the school is providing guided home learning, how they can keep their children safe online, and any new developments.

Guided home learning

Guided home learning can include the following formats:

- Uploading instructions, presentations and tasks for pupils on Satchel One, with pupils posting responses
- Providing recorded teaching material in the form of audio or video tutorials
- Directing pupils to web-based resources and activities they can engage with on or offline
- Providing written feedback on work submitted via Satchel One
- Delivering live online lessons via Microsoft Teams

Teachers will select the most appropriate format for a lesson 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 ration screen time and provide a variety of learning experiences within a lesson, across the school day/week and through a scheme of work.

Protocols for staff in relation to guided home learning:

- Only use school approved platforms; do not use social media in communicating with pupils.
- Reinforce online safety messages regularly in your teaching.
- Bear in mind the current circumstances and how they are affecting children and families when setting expectations of pupils.
- Consider online safety when sharing resources – vet websites and videos/apps/software carefully and bear in mind that the home environment will not have the same content filtering systems as at school. If introducing new apps and resources, ensure these meet GDPR requirements. Contact your Head of Department for further guidance.
- When recording video presentations staff should ensure they have a safe and appropriate place with no bedrooms/inappropriate objects/personal information visible in the background.
- If concerned about online safety/resources, check with your Head of Department.
- Ensure that passwords and secure information – such as log-ins, parent contact details – are kept confidential.

- Adhere to copyright and GDPR guidelines.
- Continue to look out for signs that a child may be at risk – which may differ from typical triggers in a school environment. Report any concerns to the DSL without delay in the usual way.
- Do not provide pupils or parents with personal contact details – email, home or mobile numbers, details of web-based identities etc.
- Do not arrange to meet pupils or ask them to deliver work to your home.
- Remain professional and objective in all forms of communication with parents and pupils.
- Never ask pupils to share their passwords or ask pupils to change to another communication platform.
- Forward any ICT issues to the ICT Manager.

In relation to live online teaching (in school or at home):

- 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.
- 1:1 teaching is not permitted; all live teaching should be conducted in a whole class setting with an additional staff member present.

Reporting an online issue for staff:

- Any child protection or safeguarding concern must be reported to the DSL without delay.
- Concerns about the safety of procedures, behaviours or use of technology should be referred to the DSL.
- Routine queries about the use of apps or online materials should be addressed to your Head of Department or ICT Manager depending on the nature of the issue.
- UKSIC's Professionals Online Safety Helpline is a good source of external advice.

Protocols for pupils in relation to guided home learning:

- Always log on through your Satchel One account.
- Do not save or forward recordings, take screenshots/screengrabs or photographs, or store footage/audio of teachers.

- Follow the school rules for conduct during guided home learning lessons as if you were in school.
- If you have concerns about online safety, or if you feel you are being bullied, talk to someone you trust.

Reporting an online issue for pupils:

- Speak to a trusted adult at home.
- Contact Childline 0800 1111 or click CEOP https://www.ceop.police.uk/safety-centre/

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. Monitoring screen time is particularly important in the current circumstances.
- While children are working from home they are connected to their home broadband so their traffic doesn't go through the school's 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 pupils and teacher: parents should communicate with school/staff in the usual manner, via school email or telephone during a period of guided home learning.
- Any parent wishing to supplement the school's guided home learning with support from online companies or individual tutors should be mindful of the importance of using reputable organisations or individuals who can provide evidence that they are safe and can be trusted to have access to children – further information can be found in the sources of support below.
- Social media, networking apps and gaming platforms are particularly popular at the moment. Parents are advised to be mindful of age restrictions and to oversee their child's social media activity.
- The school will update parents on online safety matters as required. Parents are requested to heed the school's advice and contact the school if they have concerns or encounter risk online.

Reporting an online issue for parents:

- Contact the Designated Safeguarding Lead or the Deputy Designated Safeguarding Lead for any safeguarding or child protection or online safety concern.

- You can also report an incident to CEOP https://www.thinkuknow.co.uk/parents/Get-help/Reporting-an-incident/ or Report Harmful Content https://reportharmfulcontent.com/

Contact your child's Class Teacher in the usual way for routine queries about guided home learning.

Sources of support and advice

- UK Safer Internet Centre https://www.saferinternet.org.uk/ - includes a range of activities for children of different ages
- CEOP / Thinkuknow https://www.thinkuknow.co.uk/ - includes a range of home activity packs
- National Online Safety https://nationalonlinesafety.com/ - Good guides for parents and staff
- Parent Info https://parentinfo.org/ - specifically aimed at parents
- Internet Matters https://www.internetmatters.org/ - specifically aimed at parents
- Net Aware https://www.net-aware.org.uk/ - NSPCC's advice on online matters