West Hill Primary School ICT and Internet Acceptable Use Policy

Approved by:		**Date:**
Last reviewed on:	November 2022	
Next review due by:	November 2023	

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the 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
- 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 Capability Policy and Staff Code of Conduct.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- 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 2021
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

3. 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, 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

See appendix 6 for a glossary of cyber security terminology.

4. 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 section 4.2 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
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- 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
- Setting up 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
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

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.

4.1 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 Behaviour,Staff Capability, Mobile Phone Policy and Staff Code of Conduct.

Sanctions in place for unacceptable ICT use may include revoking permission to use the school's systems.

These policies are available in the Headteacher's office and in the G Drive.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

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

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes 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 contact the Headteacher in the first instance.

Requests to access files/facilities are processed by the Senior Admin Officer in conjunction with Wandsworth IT Support.

5.1.1 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. Staff should enable multi-factor authentication on their email accounts.

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

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

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 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. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

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 that contains the personal information of another person, they must inform the school's DPO immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

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 in section 4.

5.2 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
- Does not constitute 'unacceptable use', as defined in section 4
- 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 5.5). 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 mobile phone 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 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure 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 Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely.

- Wandsworth IT manage the remote access (020 8871 373/editsupport@richmondandwandsworth.gov.uk)
- Security arrangements are managed by Wandsworth IT
- Protocols for remote access – member of staff
- Staff can request remote access through the School Business Manager

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as Wandsworth IT and our DPO may require from time to time against importing viruses or compromising system security.

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.

https://westhill.wandsworth.sch.uk/about-us/policies/

5.4 School social media accounts

The school has an official Twitter and Instagram page, managed by Jenny Piccolo, Admin Officer. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 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 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

6. Pupils

6.1 Access to ICT facilities

- Computers, ipads and equipment in the school's ICT suite are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Pupils will be provided with a Microsoft Teams account linked to the school's virtual learning environment which they can access from any device by using the following URL https://www.microsoft.com/en/microsoft-teams/log-in

6.2 Search and deletion

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.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- 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
- 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
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- 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

If pupils engage in any of the above please refer to section 4.1 above.

7. Parents

7.1 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 volunteer or as a member of the PTA) 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.

7.2 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 our website and social media channels.

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 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, and for setting permissions for 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.

The School Business Manager uses a password manager to store passwords securely. Teachers will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

Staff passwords are updated every 90 days.

8.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

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.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy: https://westhill.wandsworth.sch.uk/about-us/policies/

8.4 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 School Business 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 Headteacher immediately.

Users should always log out of systems and lock their equipment when they are 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.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers but not USB drives) to access school data, work remotely, or take personal data (such as pupil information) 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 Wandsworth IT.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The school will:

- Work with governors and Wandsworth IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **'Proportionate'**: the school will verify this by auctioning and annual audit to objectively test that what it has in place is up to scratch
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up-to-date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Automatic back-ups of critical data daily and store these backups on cloud based backup systems
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Wandsworth IT and the School Business Manager.

- Make sure the School Business Manager conducts regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are.
- Develop, review and test an incident response plan with Wandsworth IT and our DPO, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our Local Authority to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

The school wireless internet connection is secured.

- We use LGFL filtering
- Parents and the public are not permitted to access the school wifi

10.1 Pupils

Explain your school's approach to the use of wifi by pupils, including:

- Wifi is available throughout the school for curriculum use
- Pupils do not have knowledge of the password
- Pupils can only access the internet with the permission of their teacher

10.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi 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 wifi 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)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The headteacher, the School Business Manager and Wandsworth IT monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The governing body is responsible for approving this policy.

12. Related policies

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff capability
- Data protection
- Remote learning
- Mobile phone
- Data Protection Policy
- Cyber Security Policy

Appendix 1: Facebook cheat sheet for staff

Don't accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile

- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
  - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our official Facebook page
- Email/text groups for parents (for school announcements and information)
- Our virtual learning platform

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Signed:	**Date:**

Appendix 2: Acceptable use agreement for KS2

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

1. ***I learn online*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use apps, sites and games if a trusted adult says I can.
2. ***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!
3. ***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.
4. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
5. ***I am careful what I click on*** – I don't click on links I don't expect to see and only download or install things when I know it is safe or has been agreed by trusted adults.
6. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
7. ***I know it's not my fault if I see or someone sends me something bad*** – I don't need to worry about getting in trouble, but I mustn't share it. Instead, I will tell someone.
8. ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
9. ***I know new friends aren't always 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. If I want to meet them, I will ask a trusted adult, and never go alone or without telling an adult.
10. ***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.
11. ***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.
12. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
13. ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.
14. ***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.
15. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, only use the ones I am allowed to use, and report bad behaviour.
16. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.
17. ***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.

18. ***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.
19. ***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 that includes

Outside school, my trusted adults are_____

Signed: _____ **Date:** _____

For parents/carers

If your parents/carers want to find out more, they can read West Hill Primary School's full Online Safety Policy http://www.westhillprimaryschool.org/our-school/school-policies/ for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). They will also have been asked to sign an AUP for parents.
~~~~~~~~~~~~~~~~~~~~~~

My name is _____

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 **KNOW** people online aren't always who they say	
5. I don't keep **SECRETS** just because someone asks me to	
6. I don't change **CLOTHES** in front of a camera	
7. I am **RESPONSIBLE** so never share private information	
8. I am **KIND** and polite to everyone	
9. I **TELL** a trusted adult if I'm upset, worried, scared or confused	
10. If I get a **FUNNY FEELING** in my tummy, I talk to an adult	

My trusted adults are:

_____ **at school**

_____ **at home**

_____

For parents/carers

To find out more about online safety, you can read West Hill Primary School's full Online Safety Policy http://www.westhillprimaryschool.org/our-school/school-policies/ for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

You can find support and online safety resources for parents at parentsafe.lgfl.net

Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors

What is an AUP?

We ask all children, young people and adults involved in the life of West Hill Primary School to sign an Acceptable Use* Policy (AUP), 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).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

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, strategyand policy as detailed in the full Online Safety Policy. https://westhill.wandsworth.sch.uk/about-us/policies/

Where can I find out more?

All staff, governors and volunteers should read West Hill Primary School's full Online Safety Policy https://westhill.wandsworth.sch.uk/about-us/policies/ for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to Lola Corsan, Computing Lead and Year 6 teacher.

What am I agreeing to?

1. I have read and understood West Hill Primary School's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and 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 Headteachers (if by an adult). They are Lisa Carmen and Anna Healy.
3. **During remote learning:**
    - **I will not behave any differently** towards students compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
    - **I will not attempt to use a personal system or personal login for remote teaching** or set up any system on behalf of the school without SLT approval.
    - **I will not take secret recordings or screenshots** of myself or pupils during live lessons.
    - **I will conduct any video lessons in a professional environment** as if I am in school. This means I will be correctly dressed and not in a bedroom / impossible to tell that it is a bedroom if this is unavoidable (e.g. even if the camera slips). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.
    - **I will complete the issue log for live lessons** if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of students
4. I understand that in past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.
5. I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the **RSHE curriculum,** as well as safeguarding considerations when supporting pupils remotely.
6. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems 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.
7. 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, including social media, e.g. by:
    - not sharing other's images or details without permission
    - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
8. 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 Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the headteachers.
9. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it and seek guidance from the DSL.
10. I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either. More guidance on this point can be found in this

Online Reputation guidance for schools and in West Hill Primary School's social media policy/guidance.

11. I agree to adhere to all provisions of the school Data Protection Policy https://westhill.wandsworth.sch.uk/about-us/policies/ at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify Gary Hipple if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.
12. I will not store school-related data on personal devices, storage or cloud platforms. USB keys are not permitted and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
13. 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.
14. 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.
15. I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
16. I will follow the guidance in the safeguarding and online-safety policies for reporting incidents: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handing 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.

17. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____

Name: _____

Role: _____

Date: _____

To be completed by Richard Johnson, SAO

I approve this user to be allocated credentials for school systems as relevant to their role.

Signature: _____

Name: _____

Role: _____

Date: _____

Appendix 5: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.

TERM	DEFINITION
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.

Appendix 6

Online Safety Audit

Curriculum, General Approach & Communication

An effective whole-school approach requires consistency, a common understanding and clear communication. Unless everyone follows a common approach, you communicate clearly with all stakeholders, and staff know what others are doing, there will be gaps. The same will apply if policies do not reflect practice. And always remember, online safety = online safeguarding = safeguarding.

Question	Fully In Place	Partial / Needs Review	Not In Place	• Evidence / details and dates • Any actions / by whom? • Add **colour highlights** for items to add to risk register *NB – we pre-filled examples / links – delete as appropriate*
APPROACH				
Approach: whole-school & safeguarding-driven – how does the school demonstrate a whole-school approach to online safety, as particularly advocated in Keeping Children Safe in Education (KCSIE), Teaching Online Safety in School (TOSIS) and subject guidance including Relationships and Sex Education and Health Education (RSHE) and Computing? – is online safety fully accepted as part of safeguarding and therefore not treated as a separate matter, in the eyes of staff, students or parents, and equally in the curriculum and communications, or reflected in incident management and staff roles and responsibilities? – are all staff aware that any discussion of online safety, whether planned or ad hoc, may lead to a disclosure and must be dealt with in line with school safeguarding procedures? – is online safety included on safeguarding reports? – does online safety have obvious involvement of the leadership team and governors? – how does the school ensure that non-specialist staff use consistent approaches and messaging? – does the school take a non-victim-blaming approach (avoiding statements such as "well you shouldn't be on social media anyway" in response to an incident or disclosure)?				It may be helpful to reference https://www.gov.uk/government/publications/teaching-online-safety-in-schools

Approach: flexible, current curriculum – how does the school combine an informed, proactive, planned approach with a flexible, reactive approach to ensure it meets changing pupil needs (e.g. as technology changes, trends develop and incidents occur, are they fed into curriculum design and staff training)? – are staff comfortable with making the most of ad hoc opportunities to discuss and learn as online safety conversations arise? – how does the school review annually that teaching is current and relevant to the setting and pupil needs and experiences? – are all the harms and issues and 'underpinning behaviours' mentioned in TOSIS and the RSHE guidance addressed throughout the year? – is particular consideration made for vulnerable students, e.g. those with SEND and other needs? – how does the school avoid overlapping teaching, e.g. covering the same issue in different subjects (e.g. RSHE and Computing)? – do you collate 'pupil voice' to ensure messaging addresses pupils' lived experiences? – do you ensure that positive experiences online are also celebrated (not just harms and negative aspects of life online)?				You may wish to reference/consult: • https://www.gov.uk/government/publications/teaching-online-safety-in-schools • https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education • https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study
Assessment – is the curriculum informed by and measured against clear outcomes, e.g. those in the UKCIS framework Education for a Connected World (or similar)? – how do you use formative and summative assessment to ensure you are aware of pupil knowledge and skills to inform teaching, and subsequently to measure progress				Education for a Connected World is available at gov.uk/government/publications/education-for-a-connected-world The SafeSkills online safety quiz tool is free for all UK schools to use and includes teacher stats safeskills.lgfl.net
Parental engagement – how do you proactively engage parents/carers? – are parents aware of the school's broad online-safety approach? – are parents aware of the latest harms and issues as well as encouraged to use safety settings on popular platforms, devices,				Resources from parentsafe.lgfl.net may be helpful here and scare.lgfl.net

games, apps and consoles? – are parents reminded of the importance of following age ratings? – do you follow a drip-feed approach to communicating with parents?				
External influences, resources and scares – are external resources always first assessed for appropriateness (age appropriate, not overly negative, scary, victim blaming etc)? – are any external purchased schemes of work/curricula carefully adapted as necessary? – what approach does the school take to reacting to online challenges, scares and hoaxes? – how are any external visitors vetted for expertise, appropriateness and safeguarding understanding?				It may be helpful to reference • scare.lgfl.net • gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes • UKCIS victim-blaming guidance *(soon to be published at time of publication of this document)* • gov.uk/government/publications/using-external-visitors-to-support-online-safety-education-guidance-for-educational-settings LGfL provides signposting to a range of themed resources at https://saferesources.lgfl.net
POLICIES & PRACTICE				
Policies – do your policies govern all online behaviour, not just when using school devices or logged into school systems and platforms? – do you have an online-safety policy (whether standalone or section within your safeguarding and child-protection policy? – do you have (note the following might be integrated into other policies and not standalone but must be very clear if so) ○ AUPs to reflect varied roles and responsibilities, e.g. different key stages, parents, staff, visitors, governors, contractors etc. (NB whilst often called "acceptable use policy", these should reflect all online behaviour). ○ Social media policy? If not, this may be included in your online safety policy but should be clear. ○ Remote learning policy (whilst covid closures are a thing of the past, remote learning systems remain in use)				Several organisations provide customisable templates, including LGfL at https://safepolicies.lgfl.net

Content & review, policy v. practice – do you consult others to populate your policy, e.g. review templates (LSCP, fellow schools, The Key, LGfL, etc)? – where you have used content or templates, have you checked it is relevant to your setting, systems and stakeholders and adapted as appropriate? – do you regularly review these policies (not just the annual governor review but with staff and pupils who can give insights into practicability)? – how do you check that policies are both followed and possible to follow (e.g. contradictions with other policies, a ban on mobile photography when there are no school cameras and photos are often required, references to systems which no longer exist)? – are new systems, platforms, processes and user behaviour/needs regularly incorporated into these 'living' documents? – are policies updated to reflect curriculum needs, behaviour and safeguarding risks and incidents in your school?				
TRAINING				
Training & CPD – do all staff receive online safety training as part of the safeguarding training schedule (at induction and start of year or mid-year for new starters)? – is the centre of expertise in online safety within the DSL team with the most in-depth training received by this team? – are regular updates given throughout the year, reflecting trends, harms and incidents in school as well as nationally? – is training appropriate to and customised for different roles and responsibilities, with extra strategic elements for SLT and governors? – does training around 'online safety' tie in with training on other areas which may not be classically associated with online safety, such as all				Free training is available from LGfL at safetraining.lgfl.net And from most LSCPs (Local Safeguarding children Partnerships) Excellent paid training is available from many organisations such as NSPCC.

the harms mentioned in KCSIE (e.g. Prevent and many others)? – do technical staff receive sufficient training on key safeguarding elements? – do non-technical staff receive sufficient training on technical aspects?				

[END OF SECTION 1]

SAFE SCHOOL SYSTEMS

Schools have a duty to provide safe school systems – this may take the form of technology for safeguarding (e.g. filtering) or safeguarding for technology (such as behaviours or settings to adopt on a particular device or platform).

It is important to remember that technology changes all the time, whether functionality, risks or appropriate settings, and there is always a balance to be struck between safety precautions and 'over-blocking', which Keeping Children Safe in Education requires schools to avoid (the 2022 version includes reference of 'regular review'). The education element is therefore key, i.e. teaching children and young people what to do when they see or experience something worrying.

SAFEGUARDING TEAMS WILL WISH TO ENGAGE WITH THEIR TECHNICAL COLLEAGUES ON THIS SECTION – PLEASE ENSURE TO REVIEW IT TOGETHER.

QUESTION	FULLY IN PLACE	PARTIAL / NEEDS REVIEW	NOT IN PLACE	• Evidence / details and dates • Any actions / by whom? • Add **colour highlights** for items to add to risk register *NB – we pre-filled examples / links – delete as appropriate*
FILTERING				
Appropriate filtering – has your provider filed a submission with the UK Safer Internet Centre to explain why your filtering is 'appropriate'? – have DSL, SLT and technical teams all read and understood this submission, including rationale, benefits and limitations and safe search settings, e.g. for web searches and YouTube?				Safer Internet Centre submissions - https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/filtering-provider-responses YouTube guidance - https://youtube.lgfl.net
Filtering training – has your technical team attended training on your filtering platform/s to understand exactly how it works, how it is set up and what the options are in order to inform a strategic filtering approach and implement DSL/SLT requirements? – has your safeguarding team also attended training to know the questions they need to ask of their technical colleagues and to understand at a high level what filtering can/should do to inform the approach?				Tech training - https://lgfl.bookinglive.com/book/add/p/23 Safeguarding training (20 minute overview) - https://lgfl.bookinglive.com/book/add/p/5
Rationale / team effort – do your technical and safeguarding teams meet to discuss your filtering needs and document your approach regarding what is allowed / not in school and the safeguarding-driven rationale? – is this up to date, reflected accurately (and updated) in policies and				

practice, including how your approach and settings do not 'over-block', and shared with parents, staff and governors and ready to show to Ofsted?				
Reporting and regular review – do you receive regular automated reports to inform safeguarding / behaviour interventions and review use of the system to keep users safe and ensure you are not overblocking (also important to ensure access to teaching & learning sites)? – who is responsible for checking these reports have been run and are being reviewed, and that they are functioning correctly? – is the system regularly reviewed to ensure appropriate access, settings and usage, including consideration of impact				e.g. Viewing top blocked sites / categories monthly will highlight trends and changes that need to be investigated or addressed by talking to students.
Safe modes / search – do you enforce safe search on search engines and block those which do not have a safe search? For YouTube, do you enforce one of the restricted modes as appropriate for your needs?				YouTube mode checked via https://youtubemode.lgfl.net YouTube settings overview at https://youtube.lgfl.net Check at the top right of the search page if Google safe search is enforced (LGfL schools request this via a DNS change)
BYOD – if you allow 'bring your own device', what measures are applied to these devices to ensure the school internet cannot be used inappropriately simply by switching to a BYOD network				NB there are many different approaches – some schools do not allow BYOD; many do or restrict it to certain groups. Some schools insist upon logging in if using the BYOD network; others where this is not possible might choose to make it much more restrictive
Devices at home – have you applied filtering to school devices when sent home with students? – given that schools cannot protect parent/child devices, do you remind parents about how to set controls on their home internet/phones/devices etc?				Web filtering for school devices at home is available from various providers including LGfL – those solutions which also have Chrome extensions can also protect children if they access a school profile on a family device See https://parentsafe.lgfl.net for support with parental control settings and other ways parents can keep their children safe online
Linked to the curriculum and safeguarding landscape				An example for Q2 in this row – if there is a spike in failed attempts to view pornographic sites, is this covered in class

– is your filtering set up and updated to reflect the online-safety messages you teach and safeguarding concerns/cases in school? – conversely, is learning from filtering findings used to inform the curriculum?				as a priority, regardless of where it may fall in the scheme of work / plan for the year?
MONITORING				
Approach – is your approach to monitoring based on a strategic and safeguarding-driven rationale that has been made in discussion between safeguarding and technical teams? – are all senior leaders, governors and staff aware of this rationale and which of the three possible approaches (or combination) outlined by the Safer Internet Centre that your school follows.				Safer Internet Centre monitoring approaches - https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring
Appropriate monitoring – if you use a pro/active technical monitoring solution, has the provider filed a submission to the UK Safer Internet Centre? – have DSL, SLT and technical teams all read and understood this submission, including rationale, benefits and limitations.				Safer Internet Centre appropriate monitoring provider submissions – https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/monitoring-providers-responses
Monitoring training – if using a pro/active solution, has your technical team attended training to understand exactly how it works, how it is set up and what the options are in order to inform a strategic approach and implement DSL/SLT requirements? – has your safeguarding team attended training to know the questions they need to ask of their technical colleagues and to understand at a high level what monitoring can/should do to inform the approach?				
System configuration, customisation and review – do your technical and safeguarding teams meet to discuss your monitoring needs and ensure systems are configured for the devices and systems you used and regularly updated/reviewed where changes are made and new devices added to ensure no devices or systems are missed? – are systems customised for your safeguarding needs – e.g. adding				

keywords that represent new concerns in your school/area or to follow students at particular risk. – is this approach documented and the system regularly reviewed to ensure appropriate access, settings and usage / do your policies reflect practice in school and are they updated when settings / approach are changed?				
Reports – if using a pro/active solution, is the system set up in such a way that you have a manageable number of captures and are not overwhelmed and therefore at risk of missing key safeguarding alerts? – do you also run reports to spot trends over time? – are concerns fed into the safeguarding systems you use to capture manual/offline safeguarding concerns to complete the safeguarding jigsaw and not kept in a separate silo?				
Other – please also consider the school devices when at-home / curriculum / BYOD questions mentioned in the filtering section above and add any aspects not already covered there.				
HOME / REMOTE LEARNING & DEVICES IN THE HOME				
School devices in the home – if you send school devices home with students, how are they protected / monitored? – do you have internet filtering/monitoring on them? – are they locked down as 'managed devices' so software cannot be un/installed except by school admins?				Web filtering for school devices at home is available from various providers including LGfL.
Live lessons (even after covid, most schools will now deliver live lessons on scheduled and unexpected days, e.g. open days, elections, snow days, broken boilers, etc.) – do you have a remote learning policy or clause in another policy that covers behaviour for pupils and staff? What key safeguarding precautions are included?				The infographic at https://remotesafe.lgfl.net has 20 safeguarding considerations for lesson livestreaming that are good precautions to have in place. Whether you use that list or not, note your high-level precautions here.

Homework / cloud platforms accessible from home (all other platforms that can be accessed at home, whether for homework or during home learning) – are these covered in policies and AUPs and regularly updated as new platforms/systems are bought? – are all systems audited to ensure that they have an audit trail, central administration not limited to one person, oversight of administrators and settings locked down where features are not required, e.g. to not allow unmonitored communications?				
GENERAL – ALL TECHNOLOGY USED IN / BY THE SCHOOL				
Safeguarding & technical collaboration and review – do safeguarding and technical teams review at least annually (or whenever significant changes are made to technology or the way the school works or new technologies are adopted), which platforms, systems and devices are used, how, what their settings allow and why, plus risks and mitigations?				State here where this review document is kept and its latest update
Communication functionality – are all platforms that include any chat function (remember that 'comments' can be used to chat, especially if they are never monitored) included in your policies, AUPs and risk assessments and locked down in the way your school wants them? – are all staff and pupils aware which platforms they can use to communicate between pupils or between staff and pupils and that they must never use accounts/emails/apps that are not approved/linked to the school?				
Technology in your policies / AUPs – are the latest school system, platforms and devices that **CAN** be used/accessed at home included in your policies/AUPs etc? – have these been updated/audited recently to ensure they are still accurate? – are the rules there possible to follow (e.g. systems named which no longer exist or "use a school camera" when they don't exist or work)?				See safepolicies.lgfl.net for template policies Consider asking staff and students what they think of policies, not just if they agree

CYBERSECURITY				
Audit & documentation (given its importance for continuity of access to systems and data for keeping children safe, schools secure and maintaining continuity of teaching & learning, cybersecurity should be audited separately) – does your school have the recommended 3 documents from the NCSC: ○ cybersecurity policy ○ risk + asset registers ○ incident response plan – are these accurate and regularly updated, read by all and reflected in practice? – would these answer the Ofsted *Inspecting Safeguarding* document's requirement for systems to protect against cybersecurity risks"?				Templates for these three documents including notes to explain to a non-technical audience are at https://elevate.lgfl.net
Technical staff – do technical staff have training on cybersecurity and report to senior leaders and governors on issues, mitigations incidents and training needs?				The NCSC questions for governors document may be helpful here – ncsc.gov.uk/information/school-governor-questions
Training – are non-technical staff given training and regular reminders on cybersecurity best-practice (passwords, phishing, reporting and more)?				NCSC non-technical training for school staff is available for free, e.g. from LGfL https://booking.lgfl.net/book/add/p/33