

Online Safety Policy



Westbury House School

January 2024

Contents

| | | |
|---|----------------------------|---|
| 1 | Regulatory Framework | 3 |
| 2 | Online Safety | 3 |
| 3 | Version Control..... | 9 |

Appendix

| | | |
|------------|---|----|
| Appendix 1 | Cyberbullying: guidance for pupils..... | 10 |
| Appendix 2 | Acceptable Use Agreement (pupils)..... | 11 |
| Appendix 3 | Acceptable Use Policy (staff)..... | 12 |
| Appendix 4 | Staff iPad Agreement..... | 16 |
| Appendix 5 | Cybercrime..... | 17 |
| Appendix 6 | Specific Considerations for Remote Learning in the event of school closure..... | 18 |
| Appendix 7 | Social Media Policy..... | 19 |
| Appendix 8 | Online Safety Audit | 25 |

1 Regulatory framework

- 1.1 This policy has regard to the following guidance and advice
 - 1.1.1 Keeping children safe in education (DfE, September 2023) (KCSIE)
 - 1.1.2 Sexting in schools and colleges: responding to incidents and safeguarding young people (UK Council for Child Internet Safety (UKCCIS), August 2016)
 - 1.1.3 The use of social media for online radicalisation, July 2015
 - 1.1.4 Prevent duty guidance for England and Wales (HM Government, December 2023)
 - 1.1.5 Teaching Online Safety in Schools, (DfE June 2019. Last update January 2023)
 - 1.1.6 UK Council for Internet Safety guidance (various)
 - 1.1.7 Meeting digital and technology standards in schools and colleges (DfE, March 2023)

2 Online Safety

- 2.1 This Online Safety Policy outlines the commitment of Westbury House School to safeguard members of our school community online in accordance with statutory guidance and best practice. This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school; this includes our EYFS. It also applies to the use of personal digital technology on the school site (where allowed).
- 2.2 Westbury House School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.
- 2.3 Westbury House School's Online Safety policy is intended to consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Safeguarding and Child Protection, Anti-bullying, Behaviour Management, Staff and Pupil Acceptable Use policies and agreements, and Social Media policies. The policy will also form part of the school's protection from legal challenge, relating to the use of ICT.
- 2.4 As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.
- 2.5 Online Safety encompasses not only Internet technologies but also electronic communications such as electronic devices and wireless technology. It highlights the need to educate children and young people about the benefits, risks and

responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences.

- 2.6 The Internet is an open communications channel, available to all. Applications such as the Web, email, blogs and social networking all transmit information over the fibres of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day. However, it needs to be used safely.
- 2.7 Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime, radicalisation, terrorism and religious extremism and racism that would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security. The aim of this policy is to ensure appropriate steps are taken to make the virtual world a safe one for all members of the school community.
- 2.8 The School will ensure that staff have appropriate training regarding online safety as per KCSIE September 2023. The growth of different electronic media in everyday life and an ever-developing variety of devices including PCs, laptops, electronic devices, webcams etc. place an additional risk on our children. All should be aware of the dangers of sexting of putting children in danger. Internet chat rooms, discussion forums or social networks can all be used as a means of contacting children and young people with a view to grooming them for inappropriate or abusive relationships.
- 2.9 The best protection is to make pupils aware of the dangers through curriculum teaching particularly Computing ,RHE/PSHE and sex education. Protection is Prevention.
- 2.10 The breath of issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
- 2.10.1 **Content:** being exposed to illegal, inappropriate or harmful content, for example pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalization and extremism.
 - 2.10.2 **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.
 - 2.10.3 **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.
 - 2.10.4 **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams. If pupils or staff feel at risk, this can be reported to the Anti-Phishing Working Group <https://apwg.org>
- 2.11 The DSL and leadership team have regard for **Online Safety within KCSIE 2023.**
- 2.11.1 The School will ensure that appropriate filtering and monitoring systems are in place when pupils and staff access school systems and internet provision. The school will

be careful to ensure that these systems do not place unreasonable restrictions on internet access or limit what children can be taught with regards to online teaching and safeguarding

- 2.11.2 The School acknowledges that whilst filtering and monitoring is an important part of schools online safety responsibilities, it is only one part of our role. Children and adults may have access to systems external to the school control such as electronic devices and other internet enabled devices and technology.
 - 2.11.3 It is recognised that with the advancement of 5G that material can be accessed by pupils. Whilst some filters provided by the school will minimize the majority of inappropriate content it is recognized that not all can be accounted for. The teaching in lessons of RHE/PSHE and within the Computing curriculum and external bodies will emphasise what is deemed appropriate or not. Close monitoring of use of electronic devices in-particular for younger pupils will be maintained. If it felt that children are in breach, measures will be put in place to ensure inappropriate content will not be downloaded and the school reserves the right of total confiscation. The police will be involved if there is any criminal element to misuse of the internet, phones or any other form of electronic media.
 - 2.11.4 The School will ensure a comprehensive whole school curriculum response is in place to enable all pupils to learn about and manage online risks effectively and will support parents and the wider school community (including all members of staff) to become aware and alert to the need to keep children safe online.
 - 2.11.5 Pupils will be encouraged to discuss openly their use of technology and anything which makes them feel uncomfortable. (If this results in child protection concerns the schools designated child protection person should be informed immediately)
 - 2.11.6 Pupils should not give out their personal details, phone numbers, schools, home address, computer passwords etc.
 - 2.11.7 Pupils should adhere to the school policy on electronic devices, which states that all items should be handed in morning registration. In the event of late arrivals, pupils should hand their electronic devices into the office.
- 2.12 Westbury House School's approach to Online Safety is **based on**:
- 2.12.1 Educating young people to be responsible users of ICT
 - 2.12.2 Guided educational use
 - 2.12.3 Regulation and control
 - 2.12.4 Working in partnership with staff and parents
 - 2.12.5 The DFE publication: Teaching online safety in schools (June 2019)
 - 2.12.6 Education for a connected world
 - 2.12.7 Vulnerable Children in a Digital World - Internet Matters
- 2.13 Scope of the Policy
- 2.13.1 The Education and Inspections Act 2006 empowers Heads, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and

empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other On-Line Safety incidents covered by this policy, which may take place out of school, but is linked to pupil membership of the school.

2.14 Responsibility Statement and Allocation of Tasks

2.14.1 The day-to-day responsibility for online safety will be delegated to **the Online Safety Officer** to include:

- (a) a leading role in establishing and reviewing the school Online policies and documents
- (b) ensuring that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place
- (c) providing training and advice for staff and parents/guardians
- (d) liaising with school ICT technical staff
- (e) receiving reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- (f) reporting regularly to the Leadership Team

2.14.2 The Head (Designated Safeguarding Lead) and Senior Leaders role within Online Safety:

- (a) The Head and Senior Leaders are responsible for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the Online Safety Officer
- (b) The Head and Senior Leaders are responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant
- (c) The Head and Senior Leaders should consider carefully the content of safeguarding related lessons or activities (including online) in PSHE/RHE, as they will be best placed to support any pupils who may be especially impacted by a lesson.
- (d) The Head and Senior Leaders will receive regular monitoring reports from the Online Safety Officer
- (e) In the event of a serious Online Safety allegation the Head (Safeguarding Officer) and Senior Leaders will ensure staff adhere to guidance laid out in

the Safeguarding Policy

2.14.3 The RKA representative who works for Westbury House School is responsible for ensuring:

- (a) that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- (b) that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- (c) that the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- (d) that they keep up to date with On-Line Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Officer for investigation
- (e) that monitoring software / systems are implemented and updated as agreed In school policies
- (f) that appropriate handover that is given in circumstances of staff change or termination of contract

2.15 Staff and support staff

2.15.1 Staff are responsible for using the school ICT systems in accordance with the Staff Acceptable Use Policy, which they will be expected to sign before being given access to the school systems. All temporary staff will be required to sign an AUP.

2.15.2 It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- (a) A planned programme of Online Safety training will be made available to staff via Educare
- (b) All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school On-Line Safety policy and Acceptable Use Policies
- (c) The Online Safety officer will provide advice / guidance / training as required to individuals as required

2.16 Pupils

2.16.1 Pupils are responsible for using the school ICT systems in accordance with the Pupils Acceptable Use Policy, which they will be expected to sign before being given access to the school systems.

2.16.2 Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in On-Line Safety is therefore an essential part of the school's On-Line Safety provision. Children and young people need the help and support of the school to recognise and avoid On-Line Safety risks and build their resilience. It is important that we communicate with pupils in a safe and beneficial way, so that pupils remain respectfully cautious but not fearful.

2.16.3 On-Line Safety education will be provided in the following ways:

- (a) An Online Safety programme will be provided as part of Computing and RHE/PSHE, this will cover both the use of ICT and new technologies in school and outside school
- (b) Key Online Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- (c) Pupils will be taught how to evaluate what they see online so that and to be critically aware of the materials and content they access on-line and be guided to validate the accuracy and safety of information
- (d) Pupils will be taught how to recognise techniques used for persuasion by looking at false and misleading content
- (e) Staff and older pupils should act as good role models in their use of ICT, the internet and mobile devices
- (f) Pupils will also be taught how and when to seek support

2.17 Parents

2.17.1 Parents play a crucial role in ensuring that their children understand the need to use the internet and other electronic devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore offer the opportunity for Online Safety training at the beginning of each academic year. Regular Online Safety tips are included in the Head's Friday letter.

2.17.2 Parents and carers will be responsible for:

- (a) endorsing (by signature) the Pupil Acceptable Use Policy
- (b) reading the Anti-bullying policy (including On-Line Safety) which is published on the school website
- (c) attending Online Safety information evening organised by the school

2.17.3 In line with any other disciplinary incident parents will be informed of a breach of the school's bullying policy.

2.18 Data Protection

2.18.1 Personal data will be recorded, processed, transferred and made available according to the GDPR May 2018 which states that personal data must be:

- (a) Fairly and lawfully processed
- (b) Processed for limited purposes
- (c) Adequate, relevant and not excessive
- (d) Accurate
- (e) Kept no longer than is necessary
- (f) Processed in accordance with the data subject's rights
- (g) Secure
- (h) Only transferred to others with adequate protection

2.18.2 Staff must ensure that they:

- (a) At all times take care to ensure the safe-keeping of personal data, minimising the risk of its loss or misuse
- (b) Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data






3 Version control

| | |
|-------------------------------------|------------------------------------|
| Date of adoption of this policy | April 2021 |
| Date of last review of this policy | January 2024 |
| Date for next review of this policy | Autumn 2024 |
| Policy owner (SMT) | Deputy Head and Online Safety Lead |
| Policy owner (Proprietor) | ILG |

Appendix 1 Cyberbullying: guidance for pupils

- 1 Cyberbullying is bullying that takes place using technology.
- 2 Pupils should remember the following:
 - 2.1 use the security settings when using technology
 - 2.2 regularly change your password and keep it private
 - 2.3 always respect others - be careful what you say online and what images you send
 - 2.4 think before you send - whatever you send can be made public very quickly and could stay online forever
 - 2.5 if you or someone you know are being cyberbullied, **tell someone**. You have the right not to be harassed or bullied online. Tell an adult you trust - your parents, any member of staff or a helpline such as ChildLine on 0800 1111
 - 2.6 don't retaliate or reply online
 - 2.7 save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the School to investigate the matter
 - 2.8 block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly
 - 2.9 don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.
- 3 You may find the following websites helpful:
 - 3.1 <http://www.childnet.com/young-people>
 - 3.2 <https://www.thinkuknow.co.uk/>
 - 3.3 <https://www.childline.org.uk/Explore/Bullying/Pages/online-bullying.aspx>
 - 3.4 <https://www.saferinternet.org.uk/advice-centre/young-people>
 - 3.5 <https://www.disrespectnobody.co.uk/>
 - 3.6 <http://www.safetynetkids.org.uk/>
- 4 Please see the School's Acceptable Use Policy for pupils which sets out the School rules about the use of technology including mobile electronic devices.

Appendix 2 Acceptable Use Agreement (Pupil)

| | | | | | |
|--|--|--|--|--------------------------------|--|
|  WESTBURY HOUSE SCHOOL | | NAME..... CLASS..... SIGNATURE..... | | My Acceptable Use Agreement | |
| <h1>S</h1> <h2>Secret</h2>  | <h1>A</h1> <h2>Aware</h2>  | <h1>F</h1> <h2>Files & Equipment</h2>  | <h1>E</h1> <h2>Emails & Online Communication</h2>  | | |
| <ul style="list-style-type: none">-I will keep my username and password secret-I will not share personal information online with anyone unless a trusted adult has given me permission-If I am contacted by anyone I do not know, I will tell an adult straight away-I will never arrange to meet someone who I have met online | <ul style="list-style-type: none">-I must ask an adult for permission to go online-I will only use the school's computers and iPads for schoolwork and homework-I will not download anything from the internet unless I have permission from an adult-I will not visit websites and social networking sites that have age restrictions over 11-I know that my school will check on my use of apps, internet and email when I'm using devices | <ul style="list-style-type: none">-I will ask a teacher or adult if I want to use the computers or iPads-I will take care of the iPads, computers and other equipment-I will not use other people's work or pictures without permission-I will not upload files or inappropriate electronic material onto devices-I must only search for images or information which I have been asked to search for | <ul style="list-style-type: none">-I understand that a teacher or responsible adult needs to give me permission to send emails to people I don't know who we are writing to in class-I will only use my school email to send messages to teachers and pupils about school matters-I will only communicate politely online. Any messages or video calls will be kind and use no unpleasant language whether I'm at home or in school-I will not open attachments or download files unless the sender has told me to and I know and trust that person | | |

Appendix 3 Staff Acceptable Use Policy/Agreement

This policy is implemented to protect the interests and safety of the whole School community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. Whilst exciting and beneficial, both inside and outside of the context of education, many online resources are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies. We understand the responsibility to educate our pupils on online safety issues; teaching

Use of Communication Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education, compared to their risks:

| Communication Technologies | Staff and Other Adults (inc EYFS) | | | | Pupils | | | |
|--|-----------------------------------|--------------------------|----------------------------|-------------|---------|--------------------------|-------------------------------|-------------|
| | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Electronic devices may be brought to school | √ | | | | | | | √ |
| Use of electronic devices in school | | √ | | | | | √ | |
| Taking photos or videos on personal electronic devices or other camera devices | | | | √ | | | | √ |
| Use of personal email addresses in school, or on school network | | | | √ | | | | √ |
| Use of school email for personal emails | | | | √ | | | | √ |
| Use of chat rooms and social networking sites | | √ | | | | | | √ |
| Use of online instant messaging | | √ | | | | | | √ |
| Use of blogs | √ | | | | | | √ | |

Use of devices

The school provides portable IT equipment, such as laptop computers and iPads to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

Ownership

The laptop/portable device, accessories, software and operating system remain the property of the school and are provided on a loan basis. These items can and may be recalled at any time.

When a member of staff leaves the employment of the school, all equipment must be returned. It is the responsibility of the member of staff leaving to ensure that all files have been synchronised to the server and/or suitable media before the device is returned.

Before a device is re-issued to a new member of staff, all files on the local hard drive will be deleted.

The laptop/portable device is for use by the issued member of staff only. Any damage, loss or theft while in the care of a third party will result in the member of staff being liable for the cost of repair or replacement.

Responsibility

Staff should take good care of the laptop/portable device and take all reasonable precautions to ensure that it is not damaged, lost or stolen. In the event that the device is stolen, staff will be expected to report the theft to the police within 24 hours and obtain a police report for insurance purposes.

Staff members must report the loss or damage of a laptop/portable device to the School Administrator. Negligence in the care of any device or failure to report loss or damage at the earliest opportunity may result in disciplinary action being taken against the staff member concerned.

Transporting Laptops/Tablets

Laptops should always be within the protective bag/case supplied with the device when carried.

For short periods of time i.e. moving between meetings, laptops may be put into hibernation (standby mode), thus reducing the start-up time. For longer periods, laptops should be turned off properly before placing it in the carry case.

Screen Care

The laptop screen can be damaged if subject to rough treatment. The screen is particularly sensitive to damage from excessive pressure on the screen.

- a. Do not lean on the top of the laptop when it is closed.
- b. Do not place anything in the carrying case that will press against the cover.
- c. Do not place anything on the keyboard because forgetting objects on the keyboard and closing the lid may cause damage to the screen.
- d. Only clean the screen with soft, dry microfiber cloth or anti-static cloth.

Security and Storage

Staff must take appropriate security measures to protect the laptop/portable device and all its peripherals.

- Each device's serial number will be recorded in the School's inventory of IT equipment database
- Do not leave the device unattended and unsecured

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access.

Staff are permitted to bring in personal devices for their own use but are not allowed to have their phone switched on during the working day. They may use their mobile telephone only during break-times and lunchtimes. Personal telephone numbers may not be shared with pupils or parents and under no circumstances may staff contact a pupil using a personal telephone number.

Software

Staff may not install software onto a school laptop under any circumstances. If staff wish an application to be installed, they need to contact the IT Administrator (Rika).

Use of internet, email and devices inside and outside of school

Staff may not access any social networking or other websites or personal email which is unconnected with School work or business either from School devices or whilst in front of pupils. Such access may only be made from their own personal devices whilst in staff-only areas of School.

There is strong anti-virus and firewall protection on our network and, as such, it may be regarded as safe and secure. Staff should be aware that email communications may be monitored.

Staff must immediately report to the DSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any online communications will neither knowingly or recklessly:

- place a child or young person at risk of harm
- bring the School into disrepute
- breach confidentiality
- breach copyright
- breach data protection legislation; or do anything that could be considered discriminatory
- against, or bullying or harassment of, any individual, for example by: making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age
- using social media to bully another individual; or
- posting links or material which is discriminatory or offensive.

Any digital communication between staff and pupils or parents is expected to be professional in tone and content. Under no circumstances may staff contact a pupil or parent using any personal email address.

Password Security

staff have individual School network logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security. All members of staff are expected to:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed as a minimum every school year
- not write passwords down; and
- not share passwords with others

Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Care is taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute. Written permission from parents will be obtained before photographs of pupils are published on the School website or elsewhere. Photographs published on the School website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images.

I have read and understood the conditions above and agree to abide by them.

Full name (BLOCK CAPITALS):

Signature:

Date:

Appendix 4: iPad Agreement (Staff)

Personal iPad Agreement

Westbury House Preparatory School (WHS) provides Apple iPads for staff, to enable them to carry out their role more effectively. Staff provided with iPads, are asked to respect these resources and to use them appropriately.

Please sign below to accept this iPad and agree to the following terms of use:

1. This iPad remains the property of WHS and is loaned to you for use within your job role.
2. The iPad will be provided with a unique password. This password should not be shared with anyone else or disabled. Should the device be loaned to another colleague, the IT Coordinator will set up a separate user account.
3. The iPad must remain in your possession, should only be used by you and should be securely stored when not in use.
4. All iPad use must fully comply with the WHS Online Safety Policy and Data Protection Policy. Failure to do so may lead to disciplinary action.
5. The iPad is connected to your school email account so might have access to the personal information of pupils. The iPad might also be used to store personal information such as picture and video images of pupils. This means you must fully comply with high standards of data protection.
6. Loss or damage of the device should be reported to the Head immediately.
7. If it is suspected that the iPad is being inappropriately used or its whereabouts cannot be confirmed the device will be remotely locked or wiped.
8. You (and only you) may take the password protected iPad off-site if you plan to use it in a way that will benefit the school. Insurance cover provides protection from the standard risks whilst the iPad is on the school site or in your home **but excludes** theft from your car or from other establishments. Should you leave the iPad unattended and it is stolen you will be responsible for its replacement and may need to claim this from your own insurance company.
9. If you leave the employment of the school the iPad must be returned in good condition to the Head before your official leaving date.

Member of Staff:

Serial number:

I have read this agreement and fully understand that I need to adhere to all elements:

Received by Signature: Date:

Appendix 5: Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include:

- unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded
- 'Denial of Service' (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Note that Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

Additional advice can be found at: [Cyber Choices, 'NPCC- When to call the Police'](#) and [National Cyber Security Centre - NCSC.GOV.UK](#)

Appendix 6 Specific Considerations for Remote Learning in the event of school closure

1 Safeguarding

- 1.1 See Remote Learning Policy and Safeguarding and CP addendum (Sept 2020) in Staff Handbook

2 Online safety

- 2.1 Westbury House's Online Safety Leads is Claire Lowther. If the Online Safety Leads are unavailable, advice can be sought from Peter Cowley (AfC Adviser for Online Services and Safety).
- 2.2 Westbury House will continue to ensure that appropriate filters and monitoring systems are in place to protect pupils when they are online on the school's IT systems or recommended resources.
- 2.3 It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with in line with the Safeguarding and Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.
- 2.4 Westbury House will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.
- 2.5 Below are some things to consider when delivering virtual lessons, especially where webcams are involved:
 - 2.5.1 No 1:1s, groups only (with the exception of peripatetic teachers where lessons will only take place with parental supervision of the child)
 - 2.5.2 Staff (and children) must wear suitable clothing, as should anyone else in the household
 - 2.5.3 Only school email accounts and school devices should be used, not personal emails or devices
 - 2.5.4 Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred, or a suitable virtual background used
 - 2.5.5 Staff should consider privacy when allocating a workspace
 - 2.5.6 When devices are not in use, they should be locked to ensure confidential material cannot be accessed by any other party
 - 2.5.7 The live class should be recorded where reasonable possible so that if any issues were to arise, the video can be reviewed
 - 2.5.8 Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day
 - 2.5.9 Language must be professional and appropriate, including any family members in the background
 - 2.5.10 Staff should record, the length, time, date and attendance of any sessions held

Appendix 7 Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

Westbury House School recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and learners are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

Scope

This policy is subject to the school's codes of conduct and acceptable use agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and learners may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with learners are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control

Roles & Responsibilities

- **SLT and Online Safety Officer**
 - Facilitating training and guidance on Social Media use.
 - Developing and implementing the Social Media policy
 - Taking a lead role in investigating any reported incidents.
 - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
 - Receive completed applications for Social Media accounts
 - Approve account creation

- **Administrator/Moderator**
 - Create the account following SLT approval
 - Store account details, including passwords securely
 - Be involved in monitoring and contributing to the account
 - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

- **Staff**
 - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
 - Attending appropriate training
 - Regularly monitoring, updating and managing content he/she has posted via school accounts
 - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a “Friends of the school” Facebook page. Anyone wishing to create such an account must present a business case to the Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the

response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy.** Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school, respond to harmful and / or offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of online communications, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing online content are:

- Engaging
- Conversational
- Informative
- Professional

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy.** If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload learner pictures online other than via official school channels.**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Learners should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
 - Personal communications are those made via a personal online accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
 - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
 - Where excessive or inappropriate personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
 - *The school permits reasonable and appropriate access to private social media sites.*
- **Learners**
 - **Staff are not permitted to follow or engage with current or prior learners of the school on any personal social media account.** *(The school may wish to define a time period re prior learners)*

- The school's education programme should enable the learners to be safe and responsible users of social media.
- Learners are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- **Parents/Carers**
 - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
 - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
 - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

Additional Considerations

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content

- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible
- Ensure the account is set up securely and the account can be transferred to another approved staff member in the event of the account holder leaving the school.

The Don'ts

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Don't link to, embed or add potentially inappropriate content. Consider the appropriateness of content for any audience of school accounts.
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Appendix 8 Annual School Online Safety Audit and Risk Assessment

School name:

Audit conducted by:

Date:

To be reviewed on an annual basis by the safeguarding team and safeguarding governor.

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 | <ul style="list-style-type: none"> Evidence / details and dates Any actions / by whom? Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i> |
|--|----------------|------------------------|--------------|---|
| APPROACH | | | | |
| <p>Approach: whole-school & safeguarding-driven</p> <p>– 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?</p> <p>– 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?</p> <p>– 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?</p> | | | | <p>It may be helpful to reference https://www.gov.uk/government/publications/teaching-online-safety-in-schools</p> |

| | | | | |
|---|--|--|--|---|
| <p>– 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)?</p> | | | | |
| <p>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</p> | | | | <p>You may wish to reference/consult:</p> <ul style="list-style-type: none"> • 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 |

| | | | |
|---|--|--|---|
| celebrated (not just harms and negative aspects of life online)? | | | |
| <p>Assessment</p> <ul style="list-style-type: none"> – 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 | | | <p>Education for a Connected World is available at gov.uk/government/publications/education-for-a-connected-world</p> <p>The SafeSkills online safety quiz tool is free for all UK schools to use and includes teacher stats safeskills.lgfl.net</p> |
| <p>Parental engagement</p> <ul style="list-style-type: none"> – 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, 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? | | | <p>Resources from parentsafe.lgfl.net may be helpful here and scare.lgfl.net</p> |
| <p>External influences, resources and scares</p> <ul style="list-style-type: none"> – 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? | | | <p>It may be helpful to reference</p> <ul style="list-style-type: none"> • scare.lgfl.net • gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes • UKCIS victim-blaming guidance (<i>soon to be published at time of publication of this document</i>) • gov.uk/government/publications/using-external-visitors-to-support-online-safety-education-guidance-for- |

| | | | |
|--|--|--|--|
| <p>– how are any external visitors vetted for expertise, appropriateness and safeguarding understanding?</p> | | | <p>educational-settings</p> <p>LGfL provides signposting to a range of themed resources at https://saferesources.lgfl.net</p> |
| <p>POLICIES & PRACTICE</p> | | | |
| <p>Policies</p> <p>– do your policies govern all online behaviour, not just when using school devices or logged into school systems and platforms?</p> <p>– do you have an online-safety policy (whether standalone or section within your safeguarding and child-protection policy)?</p> <p>– do you have (note the following might be integrated into other policies and not standalone but must be very clear if so)</p> <ul style="list-style-type: none"> ○ AUPs to reflect varied roles and responsibilities, e.g. different key stages, parents, staff, visitors, governors, contractors etc. (NB whilst often called “acceptable <u>use</u> 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) | | | <p>Several organisations provide customisable templates, including LGfL at https://safepolicies.lgfl.net</p> |
| <p>Content & review, policy v. practice</p> <p>– do you consult others to populate your policy, e.g. review templates (LSCP, fellow schools, The Key, LGfL, etc)?</p> <p>– where you have used content or templates, have you checked it is relevant to your setting, systems and stakeholders and adapted as appropriate?</p> <p>– do you regularly review these policies (not just the annual governor review but with staff and pupils who can give insights</p> | | | |

| | | | |
|---|--|--|---|
| <p>into practicability)?</p> <ul style="list-style-type: none"> – 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 <u>in your school</u>? | | | |
| <h2>TRAINING</h2> | | | |
| <p>Training & CPD</p> <ul style="list-style-type: none"> – 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 the harms mentioned in KCSIE (e.g. Prevent and many others)? – do technical staff receive sufficient training on key | | | <p>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.</p> |

| | | | | |
|--|--|--|--|--|
| 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 | <ul style="list-style-type: none"> Evidence / details and dates Any actions / by whom? Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i> |
|---|----------------|------------------------|--------------|--|
| FILTERING | | | | |
| <p>Appropriate filtering</p> <ul style="list-style-type: none"> – 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? | | | | <p>Safer Internet Centre submissions - https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/filtering-provider-responses</p> <p>YouTube guidance - https://youtube.lgfl.net</p> |
| <p>Filtering training</p> <ul style="list-style-type: none"> – 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 | | | | <p>Tech training - https://lgfl.bookinglive.com/book/add/p/23</p> <p>Safeguarding training (20 minute overview) - https://lgfl.bookinglive.com/book/add/p/5</p> |

| QUESTION | FULLY IN PLACE | PARTIAL / NEEDS REVIEW | NOT IN PLACE | <ul style="list-style-type: none"> Evidence / details and dates Any actions / by whom? Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i> |
|--|----------------|------------------------|--------------|---|
| inform the approach? | | | | |
| <p>Rationale / team effort</p> <ul style="list-style-type: none"> – 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? | | | | |
| <p>Reporting and regular review</p> <ul style="list-style-type: none"> – 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 | | | | <p>e.g. Viewing top blocked sites / categories monthly will highlight trends and changes that need to be investigated or addressed by talking to students.</p> |
| <p>Safe modes / search</p> <ul style="list-style-type: none"> – 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? | | | | <p>YouTube mode checked via https://youtubemode.lgfl.net</p> <p>YouTube settings overview at https://youtube.lgfl.net</p> <p>Check at the top right of the search page if Google safe search is enforced (LGfL schools request this via a DNS change)</p> |

| QUESTION | FULLY IN PLACE | PARTIAL / NEEDS REVIEW | NOT IN PLACE | <ul style="list-style-type: none"> Evidence / details and dates Any actions / by whom? Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i> |
|---|----------------|------------------------|--------------|--|
| <p>BYOD</p> <p>– 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</p> | | | | <p>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</p> |
| <p>Devices at home</p> <p>– have you applied filtering to school devices when sent home with students?</p> <p>– given that schools cannot protect parent/child devices, do you remind parents about how to set controls on their home internet/phones/devices etc?</p> | | | | <p>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</p> <p>See https://parentsafe.lgfl.net for support with parental control settings and other ways parents can keep their children safe online</p> |
| <p>Linked to the curriculum and safeguarding landscape</p> <p>– is your filtering set up and updated to reflect the online-safety messages you teach and safeguarding concerns/cases in school?</p> <p>– conversely, is learning from filtering findings used to inform the curriculum?</p> | | | | <p>An example for Q2 in this row – if there is a spike in failed attempts to view pornographic sites, is this covered in class as a priority, regardless of where it may fall in the scheme of work / plan for the year?</p> |
| MONITORING | | | | |
| <p>Approach</p> <p>– is your approach to monitoring based on a strategic and safeguarding-driven rationale that has been made in discussion between safeguarding and technical teams?</p> <p>– 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</p> | | | | <p>Safer Internet Centre monitoring approaches - https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring</p> |

| QUESTION | FULLY IN PLACE | PARTIAL / NEEDS REVIEW | NOT IN PLACE | <ul style="list-style-type: none"> Evidence / details and dates Any actions / by whom? Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i> |
|---|----------------|------------------------|--------------|--|
| school follows. | | | | |
| <p>Appropriate monitoring</p> <ul style="list-style-type: none"> – 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. | | | | <p>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</p> |
| <p>Monitoring training</p> <ul style="list-style-type: none"> – 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? | | | | |
| <p>System configuration, customisation and review</p> <ul style="list-style-type: none"> – 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 | | | | |

| QUESTION | FULLY IN PLACE | PARTIAL / NEEDS REVIEW | NOT IN PLACE | <ul style="list-style-type: none"> Evidence / details and dates Any actions / by whom? Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i> |
|--|----------------|------------------------|--------------|---|
| <p>reviewed to ensure appropriate access, settings and usage / do your policies reflect practice in school and are they updated when settings / approach are changed?</p> | | | | |
| <p>Reports</p> <ul style="list-style-type: none"> – 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? | | | | |
| <p>Other</p> <ul style="list-style-type: none"> – 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 | | | | |
| <p>School devices in the home</p> <ul style="list-style-type: none"> – 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? | | | | <p>Web filtering for school devices at home is available from various providers including LGfL.</p> |
| <p>Live lessons (even after covid, most schools will now deliver live lessons on scheduled and unexpected days, e.g. open days,</p> | | | | <p>The infographic at https://remotesafe.lgfl.net has 20 safeguarding considerations for lesson livestreaming that are</p> |

| QUESTION | FULLY IN PLACE | PARTIAL / NEEDS REVIEW | NOT IN PLACE | <ul style="list-style-type: none"> Evidence / details and dates Any actions / by whom? Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i> |
|--|----------------|------------------------|--------------|---|
| 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? | | | | 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? | | | | |

| QUESTION | FULLY IN PLACE | PARTIAL / NEEDS REVIEW | NOT IN PLACE | <ul style="list-style-type: none"> Evidence / details and dates Any actions / by whom? Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i> |
|--|----------------|------------------------|--------------|---|
| <p>– 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?</p> | | | | |
| <p>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)?</p> | | | | <p>See safepolicies.lgfl.net for template policies</p> <p>Consider asking staff and students what they think of policies, not just if they agree</p> |
| CYBERSECURITY | | | | |
| <p>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: <ul style="list-style-type: none"> 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 <i>Inspecting Safeguarding</i></p> | | | | <p>Templates for these three documents including notes to explain to a non-technical audience are at https://elevate.lgfl.net</p> |

| QUESTION | FULLY IN PLACE | PARTIAL / NEEDS REVIEW | NOT IN PLACE | <ul style="list-style-type: none"> • Evidence / details and dates • Any actions / by whom? • Add colour highlights for items to add to risk register <i>NB – we pre-filled examples / links – delete as appropriate</i> |
|---|----------------|------------------------|--------------|---|
| document's requirement for systems to protect against cybersecurity risks"? | | | | |
| 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 <u>non-technical</u> 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 |