ONLINE SAFETY POLICY

Policy	Date	By	Changes Made
Created on	08/11/2019	Noah Black	
Adopted by Governors on	-	All Governors	
Frequency of review	Annually	SLT Member(s)	
Last Reviewed on	29/09/2023	Claire Nolan	Updated CEO to Principal

Contents

1. AIMS 2
2. LEGISLATION AND GUIDANCE 2
3. ROLES AND RESPONSIBILITIES 2
4. EDUCATING PUPILS AND YOUNG PEOPLE ABOUT ONLINE SAFETY 5
5. EDUCATING PARENTS/ PRIMARY GUARDIANS AND CARERS ABOUT ONLINE SAFETY6
6. CYBER-BULLYING 6
7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL 7
8. PUPILS AND YOUNG PEOPLE USING MOBILE DEVICES IN SCHOOL 8
9. STAFF USING WORK DEVICES OUTSIDE SCHOOL 8
11. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE 9
12. TRAINING 9
13. MONITORING ARRANGEMENTS 9
14. LINKS WITH OTHER POLICIES 9
15. APPENDICES 10

Appendix 1: acceptable use agreement (pupils/ young people and parents/carers) 10

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors) 11

Appendix 3: online safety training needs – self-audit for staff 12

Appendix 4: Guidance on Use of Virtual Communication and Delivery of Remote Pupil Learning 13

1. AIMS

Sheiling School aims to:

- Have robust processes in place to ensure the online safety of pupils and young people, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education 2023, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils and young peoples' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

3. ROLES AND RESPONSIBILITIES

3.1 The Board of Governors

The Board of Governors has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The Board of Governors will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is **Anthony Nowlan**.

All governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet *(See appendix 2 for further details)*

3.2 The Principal and Safeguarding Team

The Principal and the School's Safeguarding Team are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our Child protection and Adult protection policies.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal, Headteacher and Head of Care in ensuring that staff understand this policy and that it is being implemented consistently throughout the school and Children's Homes.
- Working with the Headteacher, Head of Care, Safeguarding Team, ICT managing body and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's safeguarding policies.
- Updating and delivering staff training on online safety *(appendix 3 contains a self-audit for staff on online safety training needs)*
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal, Headteacher and/or governing board

3.4 The ICT management Team

The School's ICT management team has oversight of the school provision ICT systems and facilitates; the team is made up of the following people: Noah Black, DSL; Dean Frances Hawksley, Headteacher; Sam Hembury, Head of Resource; Victoria Welsh, DDSL for Care; ICT provider Integra; Justin Davey, Principal.

The ICT management team is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's safeguarding, Staff Code of Conduct and Promoting Positive Behaviour in School/ In the Houses policies.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet *(see appendix 2),* and ensuring that pupils and young people follow the school's terms on acceptable use *(see appendix 1)*
- Working with the DSL/ Safeguarding Team to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school's safeguarding, Staff Code of Conduct and Promoting Positive Behaviour In School/In the Houses policies.

3.6 Parents/ Primary Guardians/ Carers

Parents/ Primary Guardians/ carers are expected to:

- Notify a member of staff or the DSL, Safeguarding Team of any concerns or queries regarding this policy
- Ensure their child/ young person has read, understood and agreed to the terms on acceptable use of the School's ICT systems and internet *(see appendix 1)*

Parents/ Primary Guardians/ carers can seek further guidance on keeping children and young people safe online from the following organisations and websites:

- Sheiling School E-Safety Area on the school website: https://www.sheilingschool.org.uk/e-safety-area/
- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use *(appendix 2)*.

4. EDUCATING PUPILS AND YOUNG PEOPLE ABOUT ONLINE SAFETY

Online Safety:

As stated in Keeping Children Safe in Education 2023 , as an education establishment, it is essential that children and young people are safeguarded from potentially harmful and inappropriate online material. The school strives to have an effective whole school approach to online safety protecting and educating pupils, young people and staff in the use of technology and having mechanisms in place to identify, intervene in and escalate any concerns where appropriate.

The issues classified in online safety can be categorised into four main areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

Pupils and young people will be taught about online safety as part of the curriculum; due to the individual needs of our pupils/ young people, this needs to be tailored according to their individual abilities; however generally the curriculum will cover the following areas for pupils/ young people over the curriculum:

In **Early Years Education**, pupils/ young people will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In **Middle Years and Sixth Form Education**, pupils/ young people will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Recognise inappropriate content, contact and conduct, and know how to report concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils/ young peoples' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils/ young people about this.

5. EDUCATING PARENTS/ PRIMARY GUARDIANS AND CARERS ABOUT ONLINE SAFETY

The School will raise parents/ primary guardians/ carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/ primary guardians/ carers.

Online safety will also be covered during parents' evenings or suitable parent/ guardian- forums- including Annual reviews.

If parents/ primary guardians/ carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head Teacher, Head of Care (in the residential provision) and/or the DSL and deputies.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher or Safeguarding Team.

6. CYBER-BULLYING

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Anti- Bullying Policy; Staff Code of Conduct policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils and young people understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils and young people know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The School will actively discuss cyber-bullying with pupils and young people, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying awareness and prevention, its impact and ways to support pupils and young people, as part of safeguarding training *(see section 11 for more detail)*.

The School also sends information/leaflets on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children and young people who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school's child/adult protection and Anti- bullying policies. Where illegal, inappropriate or

harmful material has been spread among pupils and young people, the School will use all reasonable endeavours to ensure the incident is contained.

The DSL/ deputies will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL/ Deputy DSL's or other members of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the School's Complaints Procedure.

7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils/ young people, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the School's ICT systems and the internet *(see appendices 1 and 2)*. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the School's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils/ young people, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. PUPILS AND YOUNG PEOPLE USING MOBILE DEVICES IN SCHOOL

During transport journeys to/ from school, with prior consent from parents/ primary guardians, pupils and young people may bring personal mobile devices along with them, but they are not permitted to use personal mobile devices during the school day.

For young people in the residential provision, the same applies with prior consent from parents/ primary guardians- namely they are permitted use of personal mobile devices in the residential provision prior to and after the school day.

Any use of digital devices in school by pupils and young people must be in line with the acceptable use agreement *(see appendix 1).* This applies as well for young people in the residential provision with personal mobile devices.

Any breach of the acceptable use agreement by a pupil/ young person may trigger disciplinary action in line with the School's Promoting Positive Behaviour in School/ in the Houses policies, which may result in the temporary confiscation of their device.

9. STAFF USING WORK DEVICES OUTSIDE SCHOOL

Staff members using a work device must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure, encrypted and password-protected, and that they do not share their passwords with others. They must take all reasonable steps to ensure the

security of their work device when using it outside School. Any USB devices containing data relating to the school must be encrypted.

When working outside of the School's site, staff should seek to only use secure Internet connections and WiFi networks and avoid using free public WiFi networks due to the risk of device and network- infiltration.

If staff have any concerns over the security of their device, they must seek advice from the ICT management team (Principal/ Head of Resource & Integra) or the Safeguarding Team.

Work devices must be used solely for work activities.

10. USE OF VIRTUAL COMMUNICATION AND DELIVERY OF REMOTE PUPIL E- LEARNING

Staff who are required to use digital device platforms for use for virtual meetings and communication are expected to adhere to the above requirements. In addition, only agreed communication platforms should be used by staff that are deemed a secure means to conduct virtual communication.

Similarly, teachers, involved parents/carers, professionals, guest speakers and other school and care staff who are authorised on behalf of the school and children's home to engage in direct communication with pupils via virtual platforms for communication and remote delivery of learning should only do so in accordance with corresponding guidance set out in appendix 4 and not before signed written Acceptable Use agreements from pupils and parents/ guardians has been obtained.

11. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil or young person misuses the School's ICT systems or internet, we will follow the procedures set out in the school's Promoting Positive Behaviour in School/ in the Houses policies as well as the Child/Adult Protection policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary or capability procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The School will consider whether incidents, which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. TRAINING

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and Safeguarding Team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also continuously update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and other safeguarding policies.

13. MONITORING ARRANGEMENTS

The DSL and deputies log behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by the DSL and the Safeguarding Team. At every review, the policy will be shared with the Board of Governors for approval.

14. LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- Child protection policy
- Adult protection policy and procedures
- Anti- Bullying Policy
- Promoting Positive Behaviour in School/ in the Houses policies
- Staff Code of Conduct Policy

- Staff disciplinary procedures
- Data Protection policy and privacy notices
- Complaints procedure

15. APPENDICES

Appendix 1: acceptable use agreement (pupils/ young people and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils/ Y.P and parents/carers

Name of pupil/ Y.P:

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during the day whilst at school
- Whilst journeying to/ from school, I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils/ young people using the school's ICT systems and internet, and for using personal electronic devices to/ from school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors
Name of staff member/governor/volunteer/visitor:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT management team know if a pupil/ young person informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils and young people in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: Guidance on Use of Virtual Communication and Delivery of Remote Pupil Learning

Sheiling School Thornbury

GUIDANCE ON USE OF VIRTUAL COMMUNICATION & DELIVERY OF REMOTE PUPIL LEARNING

CONTENTS

1. Introduction
2. Working Remotely with Pupils & Young People
3. Guidelines for Pupils and Young People Connecting to a Virtual Classroom
4. Guidelines for delivery of virtual lessons from guest teachers/ professionals to classrooms
5. Virtual Meetings Between Staff, Parents and Professionals
6. Appendices

INTRODUCTION

This guidance should be read in conjunction with the following Sheiling School policies and procedures:

- Child Protection Policy and appendices
- Adult Protection Policy and appendices
- Online Safety Policy
- Anti- Bullying Policy
- Promoting Positive Behaviour Support in School Policy and appendices
- Promoting Positive Behaviour Support in the Houses Policy and appendices
- Health & Safety Policy
- Incident, Accident and Near Miss Reporting Policy
- Incident, Accident & Concern Reporting Guidance
- Staff Code of Conduct Policy

When preparing to communicate or deliver work remotely to pupils/ young people enrolled with the school, staff must have due regard and should refresh their awareness of the school's existing policies which closely link and operate in conjunction with this guidance (see section 1 above). Staff should re-read these policies and ask a line manager or member of the provision leadership team (Education Leadership Team/ Care Management Team [ELT/CMT]) if they have any questions or are unsure about aspects between policy and practice.

1) Before commencing online communication/ delivery of work via online platform, staff need to first check that the school has signed Acceptable Use agreements from the pupil/ young person and parent/ guardian(s) (see appendix 1 for details).

2) Staff must never communicate with pupils and young people in a way which could cause alarm, distress or misunderstanding. There should be no room for ambiguity in the communication.

3) If staff are concerned about a comment made online by a pupil/ young person or the work they share, the staff member should take a screen shot and follow the school's concern procedure by report it to a member of the Safeguarding Team and then logging the concern on the School's *BehaviourWatch* system.

4) Current guidelines for residential pupils/ young people Skyping / Facetiming family members are a sound basis for acceptable behaviour during online learning sessions using visuals; staff and pupils/young people should be fully dressed and take into account the background / surroundings.

5) Staff should use a communal area, think about anything in the background that could cause concern (e.g. art work) or would identify family members / personal information, and hang a sheet behind them if necessary.

6) The teacher/ school staff member should always act as moderator and be the responsible adult, especially where a pupil/ young person may need guidance to remove items from view. If a pupil is inappropriately dressed or in an unsuitable setting (e.g. a bedroom) they must be removed from the video call and/or the virtual communication session ceases immediately.

7) Using only audio is safer than live video feed. Using pre-recorded film clips or Youtube links, established webinars or other existing resources will also be preferable to a live video session.

8) If a live video session is required, staff must ensure that the online platform for delivery is a secure one with encrypted transmission. Online platforms that the school utilise for internal communication between school colleagues is ***Microsoft Teams***. For external online communication the school currently endorses ***Skype for Business*** and *Zoom*. Where possible, prior to commencing live video feed sessions, the school will request that the recipient of the session downloads and installs the desired communication platform. Should an alternative platform be necessary to conduct live video session, the platform must have an encrypted transmission (private) setting and a risk assessment must be carried out with prior authorisation from a member of the provision leadership team (ELT/CMT).

9) Staff must not enter into one-to-one tuition voice or video call with an individual pupil or young person without school provision leadership team (ELT/CMT) agreement. If there is a need for single pupil interaction, please ensure that a colleague is added to the call, or that a parent/ guardian is present with the pupil/ young person.

10) Following any virtual communication session or delivery of online learning, the teacher or staff member must ensure that a written log (date/time/ duration/ with whom/ witnesses/ summary of content/ lesson delivery) is kept and available via Google-Drive for review from school provision leaders.

11) Staff should avoid as much as possible to contact pupils/ young people and pupil families from personal mobile devices. If however, due to extenuating circumstances, a staff member urgently needs to call a parent or pupil/ young person from their personal phone, the number must be withheld by dialling 141 first and a record of the call must made (e.g. an email to the provision leadership team and DSL to explain the purpose of the call and any actions taken as a result of it).

12) Home filters may block different content at a different level to the school's filtering software; if this appears to be the case for one pupil in the group the teacher/ staff member should revert to or suggest an alternative resource.

13) Take care that any material provided to pupils to watch is age and developmentally appropriate. For instance, do not ask Year 9 pupils to watch a film with a 15 rating. Although this might be justified in a classroom setting (in exceptional circumstances and with the agreement of provision leaders), it is not acceptable during remote learning activities.

14) Staff should model good online behaviour in all ways, including the language used to interact with pupils and colleagues, which should be respectful at all times.

15) School provision leaders should make clear to staff the operating times for online learning (for example, only during the normal school day); no staff member should engage with or respond to any pupil/ young person outside these times.

3 GUIDELINES FOR PUPILS AND YOUNG PEOPLE CONNECTING TO A VIRTUAL CLASSROOM SESSION

Prior to commencing any virtual classroom session or virtual communication with school staff, pupils and young people should be reminded by staff of the following:

- Always use a communal space such as a dining room, and NEVER a bedroom or exclusively private space.
- The location needs to be quiet and away from other distractions.
- Personal appearance - always be appropriately dressed, even if casual and, regardless of the time of day or night, NEVER in sleepwear or anything similar
- A clear background free from distractions or unwanted/inappropriate imagery. Ideally a blank wall - or hang a sheet behind yourself
- Always remove any personal items from any sight line that could identify other members of the family or other personal details
- Remember that mirrors could display items you are not expecting to be seen

- Check that the camera angle is straight ahead and stable
- Ensure you have a strong Wi-Fi connection to ensure quality video and audio
- Ensure you will not be interrupted – especially loudly or embarrassingly
- No staff member should try to have one to one contact with you outside times agreed with the school – if you are concerned or uncomfortable, contact your teacher/ Headteacher/ House Coordinator/ Head of Care or a member of the School Safeguarding Team

4 GUIDELINES FOR DELIVERY OF VIRTUAL LESSONS FROM GUEST TEACHERS/ PROFESSIONALS TO CLASSROOMS

At times, as part of enhancing the learning experience of pupils, class teachers may wish to invite guest teachers or guest speakers to deliver sessions/ lesson content to the class via a virtual platform. Inviting guest teachers and speakers in this manner reduces certain risks to visiting in person; however there are likewise considerations that are needed especially in relation to our pupils and staff's duty to them and their safety on a virtual platform. As such the following would need to be adhered to:

- Preparations in advance will need to be done by the teacher and initial approval by ELT as to the purpose of the lesson, who is delivering it, how long, will the guest teacher/ speaker expect to be remunerated and if so what the cost would be. ELT will then need to formally approve the delivery of the session once all necessary preparations are in place.
- Consideration needs to be given as to whether this could be delivered in a pre-recorded format and weighing the benefit both from an e-safety as well as an educational perspective. A pre-recorded session minimizes exposure of guests to direct contact with school pupils and the potential for pupil impulsive behaviours and also gives some element of control of the teacher in the segments of delivery of the content. On the other-hand, a "live" session can be more dynamic in its delivery and better engage the pupils as well as provide them with a richer educational learning experience from multiple angles.
- If this will be done as a "live" event, this needs to be risk assessed in advance by the teacher and as part of this risk assessment, a copy of this guidance must be shared in advance with the guest teacher/speaker and a written agreement must be obtained (via e-mail) by the guest that they will abide by the guidance in terms of delivery of content and presentation of delivery.
- This also includes agreement that they will not be recording the session and understanding that any support provided to the pupils will be managed by the class teacher and staff team.
- The guest teacher/ speaker must also be prepped in advance by the class teacher about the profile of need of the pupils in the class (without specific details of individual pupils given) and written agreement reached that should certain thresholds of behaviour by pupils occur that the session may need to be terminated at the discretion of the supervising class teacher.
- Finally, the class teacher and identified supporting staff must be present to supervise the session- as well as ensure that pupils adhere to appropriate behavioural expectations during the lesson.

5 VIRTUAL MEETINGS BETWEEN STAFF, PARENTS AND PROFESSIONALS

Prior to commencing any virtual meeting sessions between staff, parents and other professionals ensure that the following principles are adhered to:

1) In school use an office or one of the meeting rooms if possible. If not in a school location, always use a communal space such as a dining room, and NEVER a bedroom or exclusively private space.

2) Personal appearance- always appropriately dressed, ideally work wear.

3) A clear background free from distractions or unwanted/inappropriate imagery. Ideally a blank wall - or hang a sheet behind yourself.

4) Always remove any personal items from any sight line that could identify other members of the family or other personal details.

5) Remember that mirrors could display items you are not expecting to be seen.

6) Check that the camera angle is straight ahead and stable.

Further information and helpful guidance on these matters can also be found on the NSPCC website.

Sheiling School Thornbury

Acceptable Use for Virtual School Communication & Remote Learning: Agreement for pupils/ Y.P and parents/carers

Name of pupil/ Y.P:

When using ICT platforms for accessing the internet for school communication and off-site learning I will:

- Use them for strictly educational purpose during the session
- Use them with a responsible adult present to supervise
- Use an agreed common/family space (such as dining/ sitting room) for conducting the session
- Be dressed appropriately for the session.
- Be prepared and punctual for the session.
- Conduct myself appropriately at all times including my verbal language, general behaviour and written communication.
- Not access any inappropriate websites or content.
- Not access social networking sites, gaming, use chat rooms or engage in other unrelated activities during the session.

Signed (pupil):	**Date:**

Parent/carer agreement:

I agree that my child will use offsite ICT platforms and internet responsibly for the purposes of virtual school communication and offsite learning from school staff.

I will ensure that my child will be appropriately supervised by a responsible adult during such contact from school staff for such purposes. Furthermore, I will ensure that an appropriate physical space is provided to carry out such sessions.

I agree to the conditions set out above for pupils/ young people use of ICT platforms and internet for this specific purpose and I will make sure my child understands this and support my child to adhere to these expectations of responsible conduct.

Signed (parent/carer):	**Date:**