St Mary Redcliffe and Temple School

# Online Safety Policy (Acceptable Use Agreements)

| | | |
|---|---|---|
| **Approved by** | FGB | **Date** 27 November 2025 |
| **Last reviewed on** | November 2022 | |
| **Next review due by** | November 2026 | |

## 1. Aims

Our School aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors.
- Identify and support groups of students that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

### The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial, or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing, and/or financial scams.

## 2. Legislation and Guidance

This Policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schoolshttps://www.gov.uk/government/publications/preventing-and-tackling-bullying
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation

This Policy also refers to the DfE'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
- The Equality Act 2010.

In addition, it reflects the Education Act 2011, which gave school staff stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

This Policy also takes into consideration the National Curriculum in England: computing programmes of study.

## 3. Roles and Responsibilities

### The Governing Body

The Governing Body has overall responsibility for monitoring this Policy and holding the Headteacher to account for its implementation.

The Governing Body will:

- Ensure that all staff (including governors) undergo online safety training as part of child protection and safeguarding training, and ensure relevant staff understand their expectations, roles, and responsibilities around filtering and monitoring.
- Ensure that all staff receive regular online safety updates (via email, e-bulletins, and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- Co-ordinate regular meetings with relevant staff to discuss online safety and requirements for training, and they will monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).
- Ensure that students are taught how to keep themselves and others safe, including online.
- Ensure that the School has appropriate filtering and monitoring systems in place on School devices and network, and will regularly review their effectiveness.
- Review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:
- Identify and assign roles and responsibilities to manage filtering and monitoring systems.
- Review filtering and monitoring provisions at least annually.
- Ensure the blocking of harmful and inappropriate content without unreasonably impacting teaching and learning.
- Have effective monitoring strategies in place that meet this School's safeguarding needs.

A named governor (see committee structure) will be responsible for overseeing online safety as part of their Safeguarding responsibilities.

All governors will:

- Ensure they have read and understand this Policy.
- Agree and adhere to the terms of the Acceptable Use Agreement regarding use of our ICT systems and the internet (Appendix 2).
- Ensure that online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and/or procedures.

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

### The Headteacher

The Headteacher is responsible for ensuring that the DSL arranges appropriate training so that staff understand this Policy, and that it is being implemented consistently throughout this School.

### The Designated Safeguarding Lead (DSL)

Details of our School's Designated Safeguarding Lead (DSL) are set out in the Safeguarding Policy (add link to website) and are communicated on our website.

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

- Supporting the Headteacher in making sure that staff understand this Policy and that it is being implemented consistently throughout our School.
- Working with the Headteacher and Governing Body to review this policy annually and make sure that procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on School devices and network.
- Providing the Governing Body with assurance that filtering and monitoring systems are working effectively and are reviewed regularly.
- Working with the ICT Manager to make sure the appropriate systems and processes are in place.
- Working with the Headteacher, ICT Manager, and other staff as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the Safeguarding Policy.
- Responding to safeguarding concerns identified by filtering and monitoring.
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this Policy.
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the Behaviour and Good Relationships Policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headteacher and/or Governing Body.
- Undertaking annual risk assessments that consider and reflect the risks students face through the terms of the Acceptable Use Agreement.
- Providing regular safeguarding/child protection updates, including online safety, to all staff, at least annually, to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

### The IT Manager

The IT manager is responsible for:

- Putting in place an appropriate level of security protection, such as filtering and monitoring systems on School devices and the network, which are reviewed and updated at least annually to assess effectiveness and make sure that students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Making sure that 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 ICT systems daily.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this Policy.
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the Behaviour and Good Relationships Policy.

This list is not intended to be exhaustive.

### All staff and volunteers

All staff and volunteers are responsible for:

- Maintaining an understanding of this Policy.
- Implementing this Policy consistently.
- Agreeing and adhering to the terms of the Acceptable Use Agreement relating to School ICT systems and the internet (Appendix 2) and making sure that students follow the terms of the Acceptable Use Agreement (Appendices 1).
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes in conjunction with the IT Manager, and being aware of how to report any incidents of those systems or processes failing by emailing safeguarding@smrt.bristol.sch.uk and/or speaking to the DSL if the matter is considered urgent.
- Following the correct procedures by requesting via line managers/SLT link if they need to bypass the filtering and monitoring systems for educational purposes. This will be escalated to the DSL where necessary.
- Working with the DSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this Policy.
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the Behaviour and Good Relationships Policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

### Parents/carers

Parents/carers are expected to:

- Notify a member of the safeguarding team (safeguarding@smrt.bristol.sch.uk) of any concerns or queries regarding this Policy.

- Ensure that their child has read, understood, and agreed to the terms of the Acceptable Use Agreement relating to ICT systems and internet (Appendices 1 and 2).
- Seek further guidance on keeping children safe online from the following organisations and websites:
  - What are the issues? – UK Safer Internet Centre
  - Help and advice for parents/carers – Childnet
  - Parents/carers resource sheet – Childnet

### Visitors and members of the community

Visitors and members of the community who use our ICT systems or internet will be made aware of this Policy and expected to read and follow it. Information is available when signing in (on screen) and via the visitor safeguarding information leaflet they are given when they arrive. If appropriate, they will be expected to agree to the terms of the Acceptable Use Agreement (Appendix 2).

## 4. Educating Students about Online Safety

Students will be taught about online safety as part of the Computing and Values in Practice curriculum.

We have referred to the National Curriculum in England: computing programmes of study and the Government's guidance on Relationships education (Relationships and sex education (RSE) and health education) with regard to the following information.

In **KS3**, students 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 inappropriate content, contact, and conduct, and know how to report concerns.

Students in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

By the **end of secondary school**, all students will know:

- Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners.

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).
- The similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online.

The safe use of social media and the internet may also be covered in other subject areas, e.g. English, Pastoral Curriculum, Media Studies, etc.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse, and some students with SEND.

## 5. Educating Parents/Carers about Online Safety

We will raise parents/carers' awareness of internet safety in twice termly safeguarding updates (known as 'Wake up Wednesdays'), letters, or other communications home, and in information found on our website. This Policy will also be shared with parents/carers via the Policies page of our website.

We will let parents/carers know what their children are being asked to do online, including the sites they will be asked to access, and who from our School (if anyone) their child will be interacting with online via Values in Practice (ViP) lessons and termly ViP lesson updates

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the safeguarding team (safeguarding@smrt.bristol.sch.uk).

## 6. Cyber-Bullying

### Definition

Cyber-bullying takes place online, e.g. through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or a group by another person or group, where the relationship involves an imbalance of power.

### Preventing and addressing cyber-bullying

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

We will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups as part of the Pastoral Curriculum.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes the Values in Practice curriculum (our version of personal, social, health and economic (PSHE) education), and other subjects, e.g. Media Studies or English, where appropriate.

All staff, governors, and volunteers (where appropriate) receive training on cyber-bullying, its impact, and ways to support students, as part of safeguarding training. Refer to the Training section of this Policy for more detail.

We also send information via email/bulletins regarding cyber-bullying to parents/carers so they are aware of the signs, how to report it, and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, we will follow the processes set out in the Behaviour and Good Relationship Policy. Where illegal, inappropriate, or harmful material has been spread among students, we will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if the DSL has reasonable grounds to suspect that possessing that material is illegal. The DSL will also work with external services if it is deemed necessary to do so.

### Examining electronic devices

The Headteacher, and those staff who are Team Teach trained and authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in our Mobile Phone Policy as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other students and staff. If the search is not urgent, they will seek advice from a member of SLT and/or the DSL and/or Deputy DSLs.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about the process.
- Seek the student's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on

an electronic device, the staff member should reasonably suspect that the device has or could be used to:

- Cause harm, and/or
- Undermine the safe environment of this School or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to a member of SLT and/or the DSL and/or DSL to decide on a suitable response. If there are images, data, or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent/carer refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image.
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation.
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
- The Behaviour and Good Relationships Policy.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through our Complaints Policy.

### Artificial Intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

We recognise that AI has many uses to help students learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio, or video hoaxes that look real. This includes deepfake pornography, i.e. pornographic content created using AI to include someone's likeness. Students are introduced to this topic as part of our ViP Curriculum.

We will treat any use of AI to bully students very seriously, in line with our Behaviour and Good Relationships Policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a dynamic risk assessment where new AI tools are being used, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, students and staff.

## 7. Acceptable Use of the Internet in this School

All students, parents/carers, staff, volunteers, and governors are expected to sign an Acceptable Use Agreement that applies to the use of our ICT systems and the internet (Appendices 1 and 2). Visitors will be expected to read and agree to the terms of our Acceptable Use Agreement, where applicable.

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

We reserve the right to monitor the websites visited by students, staff, volunteers, governors, and visitors to ensure that they comply with the terms of our Acceptable Use Agreement and will restrict access through filtering systems where appropriate.

More information is set out the relevant Acceptable Use Agreement (Appendices 1 and 2).

## 8. Students Using Mobile Devices On-Site

The School has a robust Mobile Phone Policy that works in conjunction with this Policy and the Acceptable Use Agreement (included below) to ensure that students do not use mobile phones in School, except with the express position of a member of staff.

Any breach of the Acceptable Use Agreement by a student may trigger disciplinary action in line with our Behaviour and Good Relationships Policy and may result in the confiscation of their device.

## 9. Staff Using Work Devices Off-Site

All staff members will take appropriate steps to ensure that their School and personal devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager.
- Making sure the device locks if left inactive for a period.
- Not sharing a device provided by the School among family or friends.

Our Tech Support will ensue that School devices have up to date software/anti-virus software as necessary.

Staff members must not use the device in any way that would violate the terms of the Acceptable Use Agreement, as set out in Appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their School provided device, they must seek advice from the IT Manager.

## 10. How our School will Respond to Issues of Misuse

Where a student misuses our ICT systems or internet, we will follow the procedures set out in our policies (Behaviour and Good Relationships Policy and this Policy/Acceptable Use Agreement). 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 our ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with our internal staff policies and procedures. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident. We will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## 11. Training

### Staff, governors, and volunteers

All new staff, governors, and volunteers 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, governors. and volunteers 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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
  - Abusive, threatening, harassing, and misogynistic messages.
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
  - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence, and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and Deputy DSLs will undertake Level 3 child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about 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 safeguarding policy.

### Students

All students will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information.
- Password security.
- Social engineering.
- The risks of removable storage devices (e.g. USBs).
- Multi-factor authentication.
- How to report a cyber incident or attack.
- How to report a personal data breach.

Students will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

## 12. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This Policy will be reviewed annually by the DSL. At every review, the Policy will be shared with the Governing Body.

## 13. Links with Other Policies

This Policy is linked to these policies which can be found on our website:

- Safeguarding Policy
- Behaviour and Good Relationships Policy
- Data Protection Policy
- Privacy Notice
- Complaints Policy

External documentation is linked throughout this Policy.

## Appendix 1: Acceptable Use Agreement (Students and Parents/Carers)

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET AGREEMENT FOR STUDENTS AND PARENTS/CARERS | |
|---|---|
| **Name of student** | |
| **I will read and follow the rules in this Acceptable Use Agreement.**<br>**When I use the School's ICT systems (e.g. computers) and use the internet in School:**<br>**I will:**<br>• Always use the ICT systems and the internet responsibly and for educational purposes only.<br>• Only use them when a teacher is present, or with a teacher's permission.<br>• Keep my usernames and passwords safe and not share these with others.<br>• Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer.<br>• Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress, or harm me or others.<br>• Always log off or shut down a computer when I've finished using it.<br>**I will not:**<br>• Access any inappropriate websites, including social networking sites, chat rooms, and gaming sites, unless my teacher has expressly allowed this as part of a learning activity.<br>• Open any attachments in emails, or follow any links in emails, without first checking with a teacher.<br>• Use any inappropriate language when communicating online, including in emails.<br>• Create, link, to or post any material that is pornographic, offensive, obscene, or otherwise inappropriate.<br>• Log in to the network using someone else's details.<br>• Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.<br>**If I bring a personal mobile phone or other personal electronic device into School:**<br>• I will not use it during lessons, tutor time, clubs, or other activities without a teacher's permission.<br>• If I am given permission, I will use the phone/device responsibly and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online.<br>**I understand and agree that School will monitor the websites I visit and that there will be consequences if I don't follow the rules.** | |
| **Signed (student)** | **Date** |
| **Parent/carer's agreement:**<br>I agree that my child can use the School's ICT systems and internet when appropriately supervised by a member of school staff.<br>I agree to the conditions set out above for students using School's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these (see Mobile Phone Policy for further information). | |
| **Signed (parent/carer)** | **Date** |

## Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteers, and Visitors)

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS | |
|---|---|
| **Name** | |
| **When using the School's ICT systems and accessing the internet in school, or outside school on a work device (where applicable):**<br>**I will not:**<br>• Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, or pornographic nature (or create, link-to, send and/or share such material with students or other parties).<br>• Use them in any way that could harm School's reputation.<br>• Access social networking sites or chat rooms.<br>• Use any improper language when communicating online, including in emails or other messaging services.<br>• Install any unauthorised software or connect unauthorised hardware or devices to the network.<br>• Share my password with others or log in to the network using someone else's details.<br>• Take photographs of students without checking with a member of SLT/my Line Manager first<br>• Share confidential information about our School, its students or staff, or other members of the community.<br>• Access, modify, or share data I'm not authorised to access, modify, or share.<br>• Promote private businesses, unless that business is directly related to our School.<br>**I will:**<br>• 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.<br>• Agree that School will monitor the websites I visit and my use of the School's ICT facilities and systems.<br>• Take all reasonable steps to ensure that School 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.<br>• Let the Designated Safeguarding Lead (DSL) and ICT Manager know if a student informs me that they have found any material that might upset, distress, or harm them or others, and will also do so if I encounter any such material.<br>• Always use the school's ICT systems and internet responsibly and ensure that students in my care do so too. | |
| **Signed (staff member/governor/volunteer/visitor)** | **Date** |
| | |