St Mary Redcliffe and Temple School

Online Safety and Acceptable Use Policy

Approved by:	FGB	**Date:** 28 November 2022
Last reviewed on:	8 March 2023	
Next review due by:	January 2024	

Contents

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, 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, 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, fake news, 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 them 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; and
- **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 schools
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It 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 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 Students' electronic devices where they believe there is a 'good reason' to do so.

The Policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 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 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 Child in Care and Safeguarding Link Governor
All Governors will:

- Ensure that they have read and understand this Policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their 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

3.2 The Headteacher

The Headteacher is 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) are set out in our Safeguarding and Child Protection Policy as well as relevant job descriptions.
The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this Policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, IT 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 school's Safeguarding and Child Protection Policy
- Ensuring that any online safety incidents are logged (see appendix 4) 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 Behaviour and Good Relationships Policy
- 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 Headteacher and/or Governing Body

This list is not intended to be exhaustive.

3.4 The IT Manager

The IT Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT 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 IT systems on a [weekly/fortnightly/monthly] 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 (see appendix 4) 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 Behaviour and Good Relationships Policy

This list is not intended to be exhaustive.

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 IT systems and the internet (appendix 2), and ensuring that students follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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 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.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this Policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (appendix 1)

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT 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 Students about online safety

Students will be taught about online safety as part of the curriculum in line with the National Curriculum computing programmes of study.

In **Key Stage 3**, 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 **Key Stage 4** 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**, 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 which 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 which 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 safe use of social media and the internet will also be covered in other subjects where relevant. 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

The school will raise parents'/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/carers.

Online safety will also be covered during parents'/carers' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use

- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

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

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's Behaviour and Good Relationships Policy.)

6.2 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 are encouraged to do so, including where they are a witness rather than the victim.

The school 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.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Values in Practice (ViP), and other subjects 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 (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 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 Behaviour and Good Relationships Policy. Where illegal, inappropriate or harmful material has been spread among students, the school 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 they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher (as set out in our searches procedures and Safe Boundaries and Good Relationships Handbook), 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 the school rules 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:

- Make an assessment of 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 the Deputy Headteacher (Behaviour, Inclusion and Ethos), DSL or Headteacher
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's cooperation

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 the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Deputy Headteacher (Behaviour, Inclusion and Ethos), DSL or Headteacher 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 if 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 a Deputy DSL in their absence) 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

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

7. Acceptable use of the internet in school

All students, parents/carers, staff, volunteers and Governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 to 3). 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 students, 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 to 2.

8. Students using mobile devices in school

Students may bring mobile devices into school, but are not permitted to use them whilst on the school premises. Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

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

10. How the school will respond to issues of misuse

Where a student misuses the school's IT systems or internet, we will follow the procedures set out in our Policies on behaviour and IT acceptable use. 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 IT 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 procedures and Staff Code of Conduct. 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.

11. 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).

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, 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 deputies will undertake Child Protection and Safeguarding training, which will include online safety, at least every 2 years. They will also 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 Safeguarding and Child Protection Policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This Policy will be reviewed every year by the Child in Care and Safeguarding Link Governor. At every review, the Policy will be shared with the Student Achievement and Support Committee. The

review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other Policies

This Online Safety Policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour and Good Relationships Policy
- Staff disciplinary procedures
- Data Protection Policy and Privacy Notices
- Complaints Policy
- IT and Internet Acceptable Use Policy

Appendix 1: KS3, KS4 and KS5 acceptable use agreement (Students and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS	
Name of Student:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's IT systems (like computers) and get onto the internet in school I will:** • Always use the school's IT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • 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 • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • 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 • 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 • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • 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 lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • 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 and that there will be consequences if I do not follow the rules.**	
Signed (Student):	**Date:**
Parent's/carer's agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's IT systems and internet, and for using personal electronic devices in 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 IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
Name of staff member/Governor/volunteer/visitor:

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Teachers' Laptops
All members of teaching staff are provided with a laptop. This laptop remains the property of the school. This laptop is allocated to a named member of staff and they alone have responsibility for it. If another member of staff borrows the laptop, responsibility remains with the teacher to whom it was originally allocated. Only staff at the school should use the laptop.

On the teacher leaving the school's employment, the laptop must be returned to the school before the last day of service. Teaching staff taking maternity leave or on long-term sick leave must return the laptop to the IT Support team, to allow it to be re-allocated to the appropriate cover staff. When in school, and not being used, the laptop must be kept in a locker or locked drawer. The laptop must not be left in an unattended car. If there is an absolute need to do so, it must be locked in the boot/out of sight. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the school's IT Manager with evidence of adequate insurance.

When being transported, the carrying case/rucksack supplied must be used at all times. Upon approval by the school's IT Manager teaching staff may have additional educational software loaded onto the laptop by the IT Support team, but it must be fully licensed and not corrupt any software or systems already installed on the laptop and must not affect the integrity of the school network.

Teaching staff must ensure that students never use the laptop whilst logged on as a staff user. If a teacher leaves their laptop unattended they must lock the computer to prevent students accessing confidential data on the system. If any fault occurs with a laptop/PC, it should be referred immediately to the IT Support Team.

General IT Rules for all Staff
If any removable media is used on school equipment, then it must be checked to ensure it is free from any viruses. Members of staff should not attempt to significantly alter the computer settings. Members of staff must ensure that all IT equipment is used in an appropriate way. Staff must not:
• Access offensive websites or download offensive material
• Use the laptop/PC for personal use during the working school day
• Copy information from the internet that is copyright protected without the owner's permission
• Place inappropriate material onto the internet
• Send emails that are offensive or otherwise inappropriate
• Disregard responsibilities for security and confidentiality
• Download files that will adversely affect the security of the laptop/PC and school network
• Access the files of others or attempt to alter the computer settings
• Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of the school
• Open email attachments unless they come from a recognised and reputable source

Members of staff must only access the system using their own name and password, which must be kept secret. Members of staff must inform the IT Support team as soon as possible if they realise that their password is no longer secret. Members of staff must always log off the system when they have finished working.

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Members of staff should understand that the school may check their computer files and emails and may monitor the internet sites they visit using school equipment.

Members of staff should not use social networking sites, such as Facebook, with students. If you wish to set a social networking activity with students please see Nick Varney (Learning Technologist) who will help you to do so in a safe and secure e-Learning environment. Members of staff should also be careful not to share details such as personal email addresses or social media account names with students.

Members of staff should actively encourage students to use the internet and IT in general in a safe and responsible way. This includes making specific reference to e-safety in discrete lessons in ViP and Computing and also in a more general sense whenever e-learning is used. Staff should remind students about the responsible use of social networks and encourage them to report any incidents of cyber-bullying to one of the Behaviour Managers or another trusted adult.

Members of staff should keep themselves aware of developments in e-Safety by participating in relevant school-based training in this area, visiting the 'e-Safety' section of Moodle and by reading the e-Safety newsletter in the relevant section of the school website. Activity that threatens the integrity of the school IT systems, or activity that attacks or corrupts other systems, is forbidden. Members of staff who have concerns in this area should raise them immediately with their line manager or the school's IT Manager.

Members of staff must recognise that data protection laws such as GDPR require that any student data to which they have access, must be kept private and confidential, except when they are required by law or by the school to disclose such information. Where personal data is transferred outside the school it should be done so securely, including using encryption and passwords if it is transferred on a USB drive. If you access data outside school using One Drive Storage or Remote File Access, you must not save that data to the hard drive of your home computer and you must ensure that no one else in your household has access to that computer as this may constitute a breach of the GDPR regulations. You should also avoid accessing data remotely on wi-fi networks which are not secure for example, using wi-fi 'hotspots' or 'open' networks in public places. If you suspect that you have been responsible for a data breach you must report this immediately to Ian Morris (School Business Manager).

For more information on handling data securely and GDPR, please see Ian Morris

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
When using the school's IT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms for non-work purposes • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of students without checking with teachers first • Share confidential information about the school, its students or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
• I will only use the school's IT 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 and my use of the school's IT facilities and systems. • 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 IT Manager know if a student 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 IT systems and internet responsibly and ensure that students in my care do so too.	
Signed (staff member/Governor/volunteer/visitor): By agreeing and logging on the link ***https://forms.office.com/r/dFt6DL1thJ, this will record your agreement***	**Date:**

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

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways students can abuse their peers online?	
Do you know what you must do if a student 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 students and parents/carers/carers?	
Do you regularly change your password for accessing the school's IT 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?	

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**