Online safety policy

St. Mark's Catholic Primary School

Contents

---

1. Aims

St Mark's aims to:

> Have robust processes in place to ensure the online safety of pupils, 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, anti-Semitism, 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 scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 education and health education in primary schools

> 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 pupils' 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 board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board 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 Ms Lucy Rout

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 ICT systems and the internet (appendix 3)

> Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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 DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The Headteacher and Assistant Headteacher takes lead responsibility for online safety in school,

> Managing all online safety issues and incidents in line with the school child protection policy

> Work with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents

> Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

> Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs. (St Mark's subscribes to https://nationalonlinesafety.com/ which provides training/webinars, regular updates and enables SLT to track and monitor training)

The Computing Subject Leader will:

> Support the Assistant headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

> Liaise with other agencies and/or external services if necessary

> Provide regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT Contractor, Focus IT Solutions are appointed to be 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 pupils 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 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

> Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

The Headteacher and Assistant Headteacher are responsible for:

> Ensuring that any online safety incidents are logged (see appendix 5) 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 behaviour 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 ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

> Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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 behaviour 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

Parents 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 ICT systems and internet (appendices 1 and 2)

Parents 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

> Healthy relationships – Disrespect Nobody

> School subscription to - https://nationalonlinesafety.com/

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 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the Computing and Relationships education and health education curriculum:

In EYFS and **Key Stage 1**, pupils 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

Pupils in **Key Stage 2** will be taught to:

> Use technology safely, respectfully and responsibly

> Recognise acceptable and unacceptable behaviour

> Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

> That people sometimes behave differently online, including by pretending to be someone they are not

> That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

> The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

> How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

> How information and data is shared and used online

> What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

> How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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

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

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, workshops and in information via our website. Parents will also have free access to https://nationalonlinesafety.com/ as part of the school' subscription. This policy will also be shared with parents.

If parents 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils 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, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their class groups.

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, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents 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 behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

Whilst children are not permitted to use their mobile phones at school, we recognise that mobile and smart technology may be used by pupils to:

> Sexually harass their peers
>
> Share indecent images: consensually and non-consensually (often via large chat groups)
>
> View and share pornography and other harmful content

We will work in partnership with parents to manage this behaviour at school and apply our Anti-bullying and Behaviour and Relationship policy as appropriate.

The DSL 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 or other member 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*

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

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

> The DfE's latest guidance on screening, searching and confiscation

> UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

> The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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 pupils, 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, 2 and 3.

8. Pupils using mobile devices in school

Pupils are not permitted to have mobile phones in school.

If pupils require mobile phones during the journey to and/or from school, they must hand the phone to the office upon arrival to be collected at the end of the day.

Any breach of the acceptable use agreement by a pupil may result in the confiscation of their device and may trigger disciplinary action in line with the school Behaviour and Relationship policy.

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

> Any USB devices containing data relating to the school must be encrypted

> Making sure the device locks if left inactive for a period of time

> Not sharing the device among family or friends

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 Focus IT Solutions the school's appointed IT contractor

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet 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 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 procedures/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:

   o   Abusive, harassing, and misogynistic messages

   o   Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

   o   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 pupils can recognise dangers and risks in online activity and can weigh the risks up

- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL 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 child protection and safeguarding 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 headteacher and Online Safety Governor. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils 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:

> Child protection and safeguarding policy

> Behaviour and Relationship policy

> Staff disciplinary procedures

> Data protection policy and privacy notices

> Complaints procedure

St. Mark's Catholic Primary School

EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS OF EYFS AND KS1 CHILDREN

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

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 using the school's ICT systems and internet, and will make sure my child understands these.

The school has a clear Online Safety Policy published on the school website, which I understand and support.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate material.

I understand that the school can, if necessary, check my child's computer files and internet history and if there are concerns about my child's safety or behaviour they will contact me.

I will support the school in adhering to the "3 Commons" promoting safe use of the internet and social media at home. I will inform the school if I have any concerns

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

St. Mark's Catholic Primary School

KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS OF KS2 CHILDREN

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT 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 username 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'm finished working on it

I will not:

- Access any inappropriate websites including: social media 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
- 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 switch it off and hand it in on the gate when I arrive at school and collect it from the gate when I leave 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 and that there will be consequences if I don't follow the rules.

Signed (pupil):	Date:

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS OF KS2 CHILDREN

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 using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

I understand that the school has a clear Online Safety Policy published on the school website.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate material.

I understand that the school can, if necessary, check my child's computer files and internet history and if there are concerns about my child's safety or behaviour they will contact me

. I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by adhering to the "3 Commons" promoting safe use of the internet and social media at home. I will inform the school if I have any concerns.

I will not allow my child to bring a phone without completing a written request and understand that the school will not take responsibility for the device and is brought to school at the owner's risk.

I will support the school in adhering to the "3 Commons" promoting safe use of the internet and social media at home. I will inform the school if I have any concerns

Signed (parent/carer):	Date:

Please refer to our comprehensive Pupil Privacy Notice on our website or hard copy held by the school office which records how we use information about you and what we do with it

St. Mark's Catholic Primary School

The use of social networking and online media

This school asks its whole community to adhere to the *3 Commons* approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?
- We always ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.
- We are kind to others online and not rude nor upset them.

How do we show common decency online?
- We do not post comments that could be considered to be **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may also be deemed harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are liable under the law.

How do we show common sense online?
- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, we check where it is saved and are aware of our privacy settings.
- We keep private information safe and so not give our name, address of telephone number without checking with a trust adult first.
- We make sure we understand changes in use of any web sites we use.
- We ignore and/or block harassing communications and report any abuse, withholding such examples as evidence.
- We never arrange to meet anyone offline without first checking with a parent/carer, or without adult supervision.

Any actions online which may affect the school, the school's reputation or a member of the school's reputation are deemed inappropriate and will be responded to.

The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/Get-help/Reporting-an-incident/

Appendix 3: acceptable use agreement (staff)

St. Mark's Catholic Primary School

Staff Acceptable Use Agreement

This Acceptable Use Agreement covers use of digital technologies in school i.e. email, Internet, network and network resources, software, equipment and systems.

- I will not reveal my password(s) to anyone.

- I will not allow unauthorised individuals to access email / Internet / network, or other school systems.

- I will ensure all documents and data are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.

- I will not engage in any online activity that may compromise my professional responsibilities.

- I will only use approved email addresses for any school/educational business.

- I will only use approved email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.

- I will not browse, download or send material that could be considered offensive to colleagues.

- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Online Safety lead or a member of SMT.

- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.

- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff.

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption, e.g. laptops and USB drives, and that I follow school data security protocols when using any such data at any location.

- I will embed the school's online-safety curriculum into my teaching.
- I understand that all Internet/network usage can be monitored and this information could be made available to my manager on request.
- I will not access social networking sites or chat rooms on school's ICT systems.
- When using any social networking sites on personal devises I will ensure that privacy settings are set to "friends only" so that my profile is not publicly visible
- I will not accept St Mark's pupils, or parents as "friends" on a social networking site to prevent any risk of inappropriate contact
- I will not use any improper language when communicating online, including in emails or other messaging services when using the school's ICT systems and internet.
- I will report any attempts by children to initiate contact on social media.
- I will not post anything online which may affect the school, the school's reputation or a member of the school's reputation.
- I understand that the school operates a no mobile phone use on site. I will limit the use of my mobile phone/smart watches and similar devices to non-contact time/outside school hours when pupils are not present and keep such devices on silent or switched off in bags/cupboards during normal school hours.
- I will not access, modify or share data I'm not authorsied to access modify or share
- I will inform the DSL if any pupil 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 when using school ICT systems.
- I understand that failure to comply with this agreement could lead to disciplinary action
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Online Safety policies.
- I will let a designated safeguarding lead (DSL) and Online Safety Lead know if a pupil 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.

Signature .... Date ....

Full Name .... (print)

Job title ....

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR 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 (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
- 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 pupils without checking parental permissions first
- Share confidential information about the school, its pupils 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 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 and my use of the school's ICT 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 ICT manager know if a pupil 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 in my care do so too.

Signed (Governor/volunteer/visitor):	Date:

Appendix 4: online safety training needs – self audit for staff

To be completed by all staff after gaining Annual Certificate in Online Safety for Teaching Staff or Non Teaching staff (2021-22) https://nationalonlinesafety.com/

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 pupils can abuse their peers online?	
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?	

Appendix 5: 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**