



# CHRIST THE SAVIOUR C.E. PRIMARY SCHOOL



Each of you should use whatever gift you have received to serve others, as faithful stewards of  
God's grace in its various forms

*1 Peter 4:10*

## Online Safety Policy

Policy to be approved by	Full Governing Body (Standards)
Policy last reviewed	July 2023
Policy ratified and adopted by the Standards Committee	Spring 2020
Policy due for review	Summer 2026

## Introduction

### Our Vision at Christ the Saviour

Rooted in our Christian foundation, we are an aspirational community loving and serving God. We seek to recognise and develop our unique gifts in accordance with the biblical principles of inclusiveness, tolerance and love, preparing children to be educated citizens in a global world.

### Our whole school curriculum intent:

Our curriculum is delivered through high quality sequential, subject specific learning. The themes of global learning and Christian Values weave throughout our curriculum. The curriculum is creative, coherent and inclusive and enables pupils to become self-motivated, independent learners. A focus on learner contribution and critical thinking enables the development of knowledge and skills that are meaningful and relevant in a global context. Each child's unique gifts are recognised and nurtured in order to prepare our children to be educated citizens in a global world.

The teaching of online safety is extremely important to achieve our school vision and our whole school curriculum intent.

Online safety is taught explicitly throughout the school in discreet sessions, as part of our computing curriculum, in clubs such as coding clubs, in assemblies and is weaved in to our planning in all other curriculum subjects.

### The legal position:

This policy is based on the Department for Education'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](#)

[Meeting digital and technology standards in schools](#)

Responding to a harmful online challenge or online Hoax:

<https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes#Teaching-about-online-safety>

Responding to sexting/ nudes semi-nudes:

<https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-how-to-respond-to-an-incident-overview>

It also refers to the Department's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' 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](#).

## **Our Aims and Intent for Computing, including online safety**

We aim to encourage children to experience rich, deep learning experiences that balance all the aspects of computing, preparing children for the rapidly changing digital landscape of the world. We aim to demonstrate effective and safe use of online content in a variety of ways relevant to them. We strive to inspire the creativity to understand the technology we have today while also adapting with the ever evolving technology available to them.

## **Roles and responsibilities**

The **Governing Body** has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The GB will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs and the filtering and monitoring standards as provided by the designated safeguarding lead (DSL).

The **Headteacher** is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The **Designated Safeguarding Lead** takes lead responsibility for online safety in school by:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- working with the senior staff, ICT manager and other staff, as necessary, to address any online safety issues or incidents,
- Working with the senior staff and ICT manager to ensure the school is meeting the DfE's digital and technology standards
- ensuring that any online safety incidents are logged using Arbor 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 behaviour 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 GB

The **ICT manager** is responsible for:

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

**All 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 and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged using Arbor and dealt with appropriately in line with this policy
- Working with the DSL to ensure any online safeguarding incidents are logged on My Concern or reported directly to the police if the child is in immediate danger
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Reporting any unsafe online content immediately to the IT manager with the following information. This should also be reported to the DSL in the usual way.
  - Date and time of unsafe content
  - Website address if possible
  - User name of pupil
  - IP address of the chromebook

**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
- Pay regard to the online safety page of our school website which is updated regularly with new guidance and support for parents
- 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 factsheet - [Childnet International](#)

**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.

**Educating pupils about online safety**

**Appendix I** lists the E-Safety coverage document from our Computing Curriculum

Pupils will be taught about online safety as part of the wider curriculum:

In **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
- 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 where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this. Regular use of technology in all subjects provides opportunities throughout the day to reinforce the positive and safe use of technology.

Additional ways to teach about E-safety are woven throughout the curriculum:

- Each of the computing units has clear E-Safety links. An 'E-safety coverage of *Switched on Computing*' document has additional E-Safety learning outcomes for each unit.
- The E-Safety poster that features on the website is shown at the start of each lesson and linked to the scenario card they discuss (see appendix 2)
- A scenario card is used at the start of each lesson to give real, age appropriate examples of what children may face online. This is discussed and resolved before the lesson continues.
- All Chromebook wallpapers changed to show the E-Safety poster for their key stage.
- Digital leaders provide a tip of the week (website articles each week from a digital leader sharing small tips to keep safe online)
- Year 6 has extra small group workshop sessions where more real life examples are discussed.
- Safer Internet Day is celebrated each year with the theme of their choice.

## **Safeguarding children**

In line with Keeping Children Safe in Education, Christ the Saviour has a filtering system in place through LGfL and G Suite.

Schools are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access

harmful or inappropriate material from the schools IT system” however, schools will need to “be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.” Ofsted concluded in 2010 that “Pupils in the schools that had ‘managed’ systems had better knowledge and understanding of how to stay safe than those in schools with ‘locked down’ systems”. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves.”

At Christ the Saviour we aim to have a strong enough filtering system to protect pupils from harmful content but an equally strong curriculum to ensure our young people know how to respond to unsafe contact or content online.

## **Filtering**

1. The main filtering system in place at Christ the Saviour is provided through LGfL (Webscreen) for all devices on site accessing the internet via the school network.

Every website that is accessed via the network is logged at LGfL. The logs go back many months which enables us to check which websites have been accessed. This identifies devices that have accessed the website, it identifies the device by the IP address. Every device on the network has a unique IP device. Google admin console and Mac server (which allocates IP addresses on the network) and the wireless controller can then be used to confirm which device the IP address relates to.

Our intention is to restrict pupils viewing dangerous or inappropriate content but not to restrict our curriculum so staff are able to inform the curriculum lead (via a google form) if they are unable to access an educational site due to the current filters and we shall then review whether the site is appropriate and if so we can unblock the site.

2. Filtering **through our school accounts** is possible when Chromebooks are at home or if the pupils use their school account on another device at home. This is accessed through G Suite via the admin console. Google Safe Search is controlled through the Google Admin Console and filters explicit search results, this has been selected for all our devices. Additional controls have been added to pupil devices such as the incognito mode which is not allowed and pupils are not able to clear their browser history. The Google Admin Console also allows us to block individual sites that pupils may be able to access at home when using their own home network.

## **Monitoring**

We have a range of monitoring strategies and systems informed by our risk assessment and circumstances. We have refined our monitoring of online safety in the following ways as a result of the increased use of devices as a result of the Covid-19 pandemic.

### **Behaviour**

The following category has been added to our behaviour monitoring system and all incidents of inappropriate online behaviour should be logged on Arbor and dealt with in line with our Behaviour Policy.

*Unsafe Online Behaviour (e.g. looking at websites not authorised by the teacher, using inappropriate language online, using devices for anything other than educational purposes)*

### **Physical Monitoring**

To ensure pupils are using Chromebooks in the safest way in school staff following these guidelines:

1. Chromebooks should never be used for Golden Time. If teachers want to have a video as a reward this should be watched on the class screen and not individually on pupil devices.
2. Pupils should only ever have one tab open at a time. If pupils need to take part in some research then the teacher will make it explicit that they are permitting them to use a second tab for a specified amount of time.
3. Pupils are taught and reminded about their digital footprint and how all activity online is monitored; teachers should frequently ask pupils to show their browser history on their screens at the end of a session where Chromebooks are used so there is a direct sense of accountability.

### **Internet and Web Access**

It is always possible to view a child's browser history on a school chromebook as the use of incognito mode and the users ability to delete their browser history is disabled.

Additional non educational websites such as discord, roblox and tiktok which are blocked by the LGfL filter in school have been blocked through the Google Admin settings on all school accounts to ensure that school devices at home are not used only for recreational purposes.

### **Proactive technology monitoring service, Securus:**

A cloud based online safeguarding and monitoring software 'Securus' helps us monitor pupils' online activity through their school accounts. This monitoring system enables us to provide early intervention for pupil safeguarding issues and help us to support pupils to learn from their mistakes quickly and safely.

### **Browsing**

Pupils are not permitted to browse the internet using the Google Search engine on their school chromebooks. If staff require children to carry out research then a link or multiple links will be shared with the children to specific sites and these can be accessed via this link.

### **Educating parents about online safety**

The school will raise parents' awareness of internet safety in emails or other communication home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher.

### **Cyber-bullying**

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.)

### **Preventing and addressing cyber-bullying**

To help prevent cyber-bullying, we ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We 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. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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.

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.

### **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

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

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

### **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 (see appendix). 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 the appendices.

### **Pupils using mobile devices in school**

Pupils in Years 5 and 6 may bring a 'brick' mobile device into school, but are not permitted to use them during:

- School hours
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

### **Staff using work devices outside school**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use. Please see our [ICT user agreement Policy](#).

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. No USB devices should be used to contain data relating to the school. Google drive must be the only means of managing data relating to the school.

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

Work devices must be used solely for work activities.

### **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 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.

### **Training**

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

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

The DSL 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.

## Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaints procedure

ICT and internet acceptable use policy

## Appendix I

E-Safety coverage document


Year 1	Title	Unit Summary	Learning outcomes for E-Safety	Programme of Study statement
Autumn	We are treasure hunters	Using programmable toys	<ul style="list-style-type: none"> <li>• learn to use simple programmable toys safely and responsibly</li> </ul>	<ul style="list-style-type: none"> <li>• use technology safely and respectfully</li> </ul>
Spring	We are collectors	Finding images using the web	<ul style="list-style-type: none"> <li>• search the internet for images, learning how to use the internet safely, as well as showing respect for others' intellectual property through observing copyright conditions</li> <li>• learn to turn the screen off and tell their teacher if they encounter material that concerns them</li> </ul>	<ul style="list-style-type: none"> <li>• use technology safely and respectfully</li> </ul>
Summer	We are celebrating	Creating a card electronically	<ul style="list-style-type: none"> <li>• learn to turn the screen off and tell their teacher if they encounter material that concerns them</li> <li>• consider the aspects of using email safely, including protecting their identity and copyright</li> </ul>	<ul style="list-style-type: none"> <li>• identify where to go for help and support when they have concerns about content on the internet or other online technologies</li> <li>• use technology safely and respectfully</li> </ul>
Year 2	Title	Unit summary	Learning outcomes for E-Safety	Programme of Study statement
Autumn	We are astronauts	Programming on screen	<ul style="list-style-type: none"> <li>• alert their teacher if they encounter inappropriate material when they search the web</li> <li>• learn about copyright and permissions</li> </ul>	<ul style="list-style-type: none"> <li>• use technology safely and respectfully</li> </ul>
Spring	We are photographers	Taking, selecting and editing digital images	<ul style="list-style-type: none"> <li>• consider implications of posting photos online</li> </ul>	<ul style="list-style-type: none"> <li>• use technology safely and respectfully</li> <li>• learn to keep personal</li> </ul>

				information private
Summer	We are detectives	Communicating clues	<ul style="list-style-type: none"> <li>• learn about the risks associated with email, including viruses and spam.</li> <li>• consider the importance of keeping personal information, including account details and passwords, private</li> </ul>	<ul style="list-style-type: none"> <li>• use technology safely and respectfully</li> <li>• learn to keep personal information private</li> </ul>
<b>Year 3</b>	<b>Title</b>	<b>Unit summary</b>	<b>Learning outcomes for E-Safety</b>	<b>Programme of Study statement</b>
Autumn	We are programmers	Programming an animation	<ul style="list-style-type: none"> <li>• consider copyright when sourcing images</li> <li>• develop safe search habits</li> <li>• consider positive participation in an online community</li> </ul>	<ul style="list-style-type: none"> <li>• use technology respectfully and safely</li> <li>• use search technologies effectively</li> </ul>
Spring	We are communicators	Communication safely on the internet	<ul style="list-style-type: none"> <li>• think about the safe use of email</li> <li>• learn about the use of video conferencing</li> </ul>	<ul style="list-style-type: none"> <li>• use technology safely, respectfully and responsibly</li> </ul>
Summer	We are presenters	Videoining performance	<ul style="list-style-type: none"> <li>• obtain filming permission and discuss implications of making the video available online</li> </ul>	<ul style="list-style-type: none"> <li>• use technology respectfully and safely</li> </ul>
<b>Year 4</b>	<b>Title</b>	<b>Unit summary</b>	<b>Learning outcomes for E-Safety</b>	<b>Programme of Study statement</b>
Autumn	We are software developers	Developing a simple educational game	<ul style="list-style-type: none"> <li>• consider copyright when sourcing images or media</li> <li>• develop safe search habits</li> </ul>	<ul style="list-style-type: none"> <li>• use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content</li> </ul>
Spring	We are musicians	Producing digital music	<ul style="list-style-type: none"> <li>• consider copyright when sourcing audio or publishing their own compositions</li> <li>• discuss illegal downloading and sharing of copyrighted music</li> </ul>	<ul style="list-style-type: none"> <li>• use technology safely, respectfully and responsibly</li> </ul>
Summer	We are co-authors	Producing a wiki	<ul style="list-style-type: none"> <li>• consider strategies for evaluating the reliability of online content</li> <li>• develop a shared wiki, thinking carefully about how to do so safely and responsibly, and considering what conduct is appropriate</li> </ul>	<ul style="list-style-type: none"> <li>• be discerning in evaluating content</li> <li>• use technology safely, respectfully and responsibly</li> </ul>
<b>Year 5</b>	<b>Title</b>	<b>Unit summary</b>	<b>Learning outcomes for E-Safety</b>	<b>Programme of Study statement</b>
Autumn	We are bloggers	Sharing experiences and opinions	<ul style="list-style-type: none"> <li>• consider what constitutes acceptable behaviours when commenting on others' blog posts</li> <li>• discuss the importance of moderating comments on blog sites</li> </ul>	<ul style="list-style-type: none"> <li>• use technology safely, respectfully and responsibly</li> <li>• be discerning in evaluating content</li> </ul>
Spring	We are web developers	Creating a web page about cyber safety	<ul style="list-style-type: none"> <li>• consider the reliability and bias of online content</li> <li>• learn how to contribute positively to a shared resource</li> </ul>	<ul style="list-style-type: none"> <li>• be discerning in evaluating content</li> <li>• recognise acceptable/unacceptable behaviour</li> <li>• use technology safely, respectfully and responsibly</li> </ul>
Summer	We are game developers	Developing an interactive game	<ul style="list-style-type: none"> <li>• consider copyright when sourcing images or media</li> <li>• develop safe search habits</li> <li>• think about how to participate positively in an online community, as well as obtaining parental permission.</li> </ul>	<ul style="list-style-type: none"> <li>• use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content</li> <li>• recognise acceptable/unacceptable behaviour</li> <li>• identify a range of ways to</li> </ul>

				report concerns about content
Year 6	Title	Unit summary	Learning outcomes for E-Safety	Programme of Study statement
Autumn	We are app planners	Planning the creation of a mobile app	<ul style="list-style-type: none"> <li>consider implications of the capabilities of smartphones and tablet computers; including how they can be used to record and share information</li> <li>learn to use search engines safely and effectively</li> </ul>	<ul style="list-style-type: none"> <li>use search technologies effectively</li> <li>use technology safely, respectfully and responsibly</li> </ul>
Spring	We are interface designers	Designing an interface for an app	<ul style="list-style-type: none"> <li>think carefully about copyright in relation both to sourcing and creating their own digital content and user interface components for their apps</li> </ul>	<ul style="list-style-type: none"> <li>use technology respectfully</li> </ul>
Summer	We are app developers	Developing a simple mobile phone app	<ul style="list-style-type: none"> <li>participate in online communities in a safe, responsible and respectful manner</li> <li>consider any safety implications for the site's users</li> </ul>	<ul style="list-style-type: none"> <li>recognise acceptable/unacceptable behaviour</li> <li>use technology safely, respectfully and responsibly</li> </ul>

## Appendix 2

Example of the 'real life' scenario cards

 <p>The screenshot shows a tweet from a user named 'Ex Ample' (@FakeExAmple) who is followed. The tweet text is 'I hate school, its so hard and everyone is so annoying!!!'. It was posted at 6:33 PM on 26 Dec 2018. The tweet has 75 retweets and 538 likes. There are icons for replies (64), retweets (75), likes (538), and direct messages.</p>	<p><b>This message is posted out of frustration. Who could it hurt? Why might it be embarrassing?</b></p> <p><b>Things to think about:</b></p> <ul style="list-style-type: none"> <li><b>Who can see my tracks?</b> When you share something online, who can see it? Think about who you're sharing with and whether they'll take care of what you share.</li> <li><b>Am I giving away too much?</b> The more you share, the more people can learn about you. Could they use your posts to be unkind to you?</li> <li><b>Does it hurt, embarrass or offend others?</b> It's important to think about whether what you post online could hurt others. Could that jokey comment you posted hurt someone's feelings?</li> </ul>
---	--

## **Appendix 3**

### **IT User Agreement, Staff and Visitors**

#### **Content**

##### **1. Aims**

- a.** This agreement covers the use of all digital technologies while in school: i.e. email, internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, apps and other relevant digital systems provided by the school or other information or systems processors
- b.** It covers school issued equipment (as logged on the asset register) when used outside school, use of online systems provided by the school such as VPN or webmail, or other systems providers when accessed from outside school
- c.** It covers posts made on any non-school official social media platform or app, made from outside the school premises or school hours which reference the school or which might bring staff members or governors professional status into disrepute
- d.** The school regularly reviews and updates they are consistent with current school policies as listed at the end of the agreement

##### **2. User Requirements**

- a.** School employees, governors, and third party staff using school systems must comply with the requirements below. Failure to do so could result in disciplinary action
- b.** School systems and users are monitored to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may be subject to monitoring
- c.** Use the school's ICT resources and systems for professional purposes or for uses deemed 'reasonable' by the Head in the line of employment
- d.** Set strong passwords and change them regularly. Do not allow others to use your accounts or know your password
- e.** Do not accept the use of anyone else's account, login or password

- f.** Do not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system via the school or other authority or processing system
- g.** Ensure all documents, data, etc. are printed, saved, accessed, deleted or shredded in accordance with the school's network and data security protocols, and retention policy
- h.** Do not engage in any online activity that may compromise professional responsibilities
- i.** Restrict school-related communication to the school's email system
- j.** Use approved methods of communicating with pupils or parents and will only communicate with them in a professional manner and on appropriate school business
- k.** Do not support or promote extremist organisations, messages or individuals
- l.** Do not give a voice or opportunity to extremist visitors with extremist views
- m.** Do not browse, download or send material that is considered offensive or of an extremist nature by the school
- n.** Report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the head
- o.** Do not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- p.** Check copyright and do not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission
- q.** Do not connect any device to the network 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 and other malware systems
- r.** Do not store any school data on a removable storage device such as a USB stick or external hard drive
- s.** Use personal cameras or phones only in line with the *Use of Digital Media and Images* in school policy
- t.** Follow the school's policy on use of mobile phones in school
- u.** If mobile phones are used for email - make sure the mobile is password protected
- v.** Use school approved equipment for any storage, editing or transfer of digital images, save photographs and videos of children and staff on the appropriate system or staff-only drive within school
- w.** Take images of staff and students with their permission and in accordance with the school's policy on the use of digital images. Do not publish any photos without permission.
- x.** Images published on the school website, online learning environment etc. will not identify students by name, or other personal information

- y.** Use the school's online cloud storage service in accordance with school protocols. If using Google Drive on a portable device, ensure the device has a lock code or pin
- z.** Ensure that any private social networking sites / blogs, etc are not confused with your professional role - create a distinction between the two
- aa.** Ensure any social networking sites are used securely so as not to compromise professional role
- bb.** Agree and accept that any computer or laptop loaned to you by the school, is provided solely to support your professional responsibilities and that you will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- cc.** Do not download any additional software without informing a member of SLT
- dd.** Access school resources remotely (such as from home) using the school approved system and follow e-security protocols to interact with them
- ee.** Ensure any confidential data that you wish to transport from one location to another is protected by encryption and that you follow school data security protocols when using any such data at any location
- ff.** Understand that data protection policy requires that any information seen by you with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that you are required by law to disclose such information to an appropriate authority
- gg.** Be aware that under the provisions of the Data Protection Act, you and the school have extended responsibilities regarding the creation, use, storage and deletion of data, and you will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage
- hh.** Understand it is your duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which you believe may be inappropriate or concerning in any way, to the relevant Senior Member of Staff / Designated Safeguarding Lead
- ii.** Understand that all internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request
- jj.** Understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes
- kk.** Understand that you have a responsibility to uphold the standing of the teaching profession and of the school, and that your digital behaviour can influence this

### **3. Links with Other Policies**

I understand that this user agreement is linked to the schools:

- Freedom of information publication scheme
- Online and E-Safety Policy
- Email Security and Etiquette Guidance
- Data Protection Policy
- Document Retention Policy
- Breach Management Policy
- Asset Management Recording Policy
- Disaster Recovery/Business Continuity Planning and Risk Register.
- Safeguarding and Child Protection Policy

#### **4. Agreement Form**

I agree to abide by these procedures and policy.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible ICT user'.

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 / safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.



## Appendix 4:

### EYFS and KS1 acceptable use agreement (pupils and parents)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents

**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
- I will 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 for using personal electronic devices in school, and will make sure my child understands these.

**Signed (parent/carer):**

**Date:**

## Appendix 5: KS2 acceptable use agreement (pupils and parents)

### Acceptable use of the school's ICT systems and internet: agreement for pupils and parents

**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 or at home I will:**

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher or adult at home 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 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 'brick' mobile phone into school:**

- I will not use it during the school day, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly

**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's 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.

**Signed (parent/carer):**

**Date:**

**Appendix 6: online safety training needs – self audit for staff**

online safety training needs audit	
<b>Name of staff member/volunteer:</b>	<b>Date:</b>
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

