Godstone Primary and Nursery School

Online Safety Policy

REVIEW DATE: September 2026

REVIEWED BY: Headteacher

NEXT REVIEW: September 2027

WRITTEN BY: Emily Boden

Contents

1. Aims 2
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating pupils about online safety 6
5. Educating parents/carers about online safety 8
6. Cyber-bullying 9
7. Acceptable use of the internet in school 13
8. Pupils using mobile devices in school 13
9. Staff using work devices outside school 13
10. How the school will respond to issues of misuse 14
11. Training 14
12. Monitoring arrangements 15
13. Links with other policies 15
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers) 14
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers) 14
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) 15
Appendix 4: YouTube Policy 16

---

1. Aims

Godstone Primary and Nursery School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. Pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. By equipping our pupils with the knowledge needed, they will be able to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

Our school aims to:

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

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, 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 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 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 and the UK Council for Internet Safety Education for a Connected World - 2020 edition framework.

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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing body will also make sure all staff receive regular online safety updates (via e-mail, e-bulletins, inset day training and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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 governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with SoftEgg staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor with responsibility for overseeing online safety (*as safeguarding governor*) is Liam McGivern.

All governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college 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 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 designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the governing body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with SoftEgg to make sure the appropriate systems and processes are in place
- Working with SoftEgg 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 child protection and safeguarding policy
- Ensuring that any online safety incidents are logged on CPOMS 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 (*appendix 4 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 DSL meetings
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager (SoftEgg)

The ICT manager (SoftEgg) 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 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 as required
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy (supported by DSLs)
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy (supported by staff)

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*)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Following the correct procedures by speaking to SoftEgg if they need to bypass the filtering and monitoring systems for educational purposes. These logs are saved and passed onto the DSLs with

reasons why the bypass has happened. SoftEgg will use the full URL for these rather than giving permission for the whole website access

- Working with the DSL to ensure that any online safety incidents are logged on CPOMS 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/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 ICT systems and internet (*appendices 1 and 2*)

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

- Internet Matters Provides age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world
- Childnet Offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support
- CEOP Education Provides information, guidance and resources for support for parents and carers, helping them to protect their child(ren) from online sexual abuse
- UK Safer Internet Centre To report and remove harmful online content

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 have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage.

As they grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own and other's online behaviour and develop effective strategies for staying safe and making a positive contribution online.

Pupils are taught about online safety as part of the curriculum. *Education for a Connected World* enables the development of teaching and learning, as well as guidance to support children and young people to live knowledgeably, responsibly and safely in a digital world. This framework therefore both supports and broadens the provision of online safety education, so that it is empowering, builds resilience and effects

positive culture change. The objectives promote the development of safe and appropriate long-term behaviours, and supports us to shape the culture within our setting and beyond.

Education for a Connected World focuses specifically on eight different aspects of online education:

1. **Self-image and Identity**

   This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and media influence in propagating stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.

2. **Online relationships**

   This strand explores how technology shapes communication styles and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships, respecting, giving and denying consent and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.

3. **Online reputation**

   This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.

4. **Online bullying**

   This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation.

5. **Managing online information**

   This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation of data, the recognition of risks and the management of online threats and challenges. It explores how online threats can pose risks to our physical safety as well as online safety. It also covers learning relevant to ethical publishing.

6. **Health, wellbeing and lifestyle**

   This strand explores the impact that technology has on health, well-being and lifestyle e.g., mood, sleep, body health and relationships. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.

7. **Privacy and security**

   This strand explores how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.

8. **Copyright and ownership**

   This strand explores the concept of ownership of online content. It explores strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

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
- 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, where relevant. Additionally, the computing lead leads monthly online safety assemblies, during which the eight strands are covered.

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

Pupils, where appropriate, are directed towards and informed about the following websites as a means of further online support both within and outside of school:

- Childline
- UK Safer Internet Centre
- CEOP Safety Centre

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters, newsletters and via the website. A copy of this policy will be available for parents/carers on the school website.

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

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

- Internet Matters Provides age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world
- Childnet Offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support
- CEOP Education Provides information, guidance and resources for support for parents and carers, helping them to protect their child(ren) from online sexual abuse
- UK Safer Internet Centre To report and remove harmful online content

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 DSLs.

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

6. Cyber-bullying

6.1 Definition

Cyberbullying, or online bullying, can be defined as the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else (see *Behaviour Policy*). Cyberbullying takes place online through, but not limited to, social networking sites, messaging apps and gaming sites.

6.2 Understanding cyber-bullying

Cyberbullying is often linked to discrimination, including on the basis of gender, race, faith, sexual orientation, gender identity or special educational needs and disabilities. For example, girls report experiencing a higher incidence of cyberbullying than boys, and lesbian, gay, bisexual and transgender people are more likely to experience bullying, including cyberbullying.

Cyberbullying, like other forms of bullying, affects self-esteem and self-confidence and can affect mental health and wellbeing, in the worst cases leading to self-harm and suicide. Addressing all forms of bullying and discrimination is vital to support the health and wellbeing of all members of the school community.

Cyberbullying takes different forms: threats and intimidation; harassment or stalking (e.g. repeatedly sending unwanted texts or instant messages); vilification and defamation; ostracism and peer rejection; impersonation; and forwarding or publicly posting private information or images.

Cyberbullying can be characterised in several specific ways that differ from face-to-face bullying. These include the profile of the person carrying out the bullying; the location of online bullying; the potential audience; the perceived anonymity of the person cyberbullying; motivation of the person cyberbullying; and the digital evidence of cyberbullying.

For the majority of people, most experiences of technology are useful and positive. Research figures vary but indicate that around 10% of young people have experienced cyberbullying. Cyberbullying can affect and involve all members of the school community – pupils, staff, parents and carers.

Every school must have measures in place to prevent all forms of bullying, including cyberbullying. School governing bodies and proprietors are required to ensure children are taught about online safety though teaching and learning opportunities.

There is not a criminal offence called cyberbullying. However, there are criminal laws that apply to a range of behaviours linked to cyberbullying including stalking, threats, accessing computer systems without permission, and circulating sexual images.

6.3 Preventing cyberbullying

To help prevent cyberbullying:

- A member of the senior leadership team takes overall responsibility for the school's work. The whole school community will need to be involved in prevention activities.
- Safeguarding and promoting the welfare of children is everyone's responsibility. All school staff are required to undertake regularly updated safeguarding and child protection training, which includes understanding, preventing and responding to cyberbullying. 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*).
- Awareness-raising and promoting understanding about cyberbullying are essential to enable ongoing discussion and to ensure members of the community are not unknowingly facilitating cyberbullying because of a lack of understanding.
- Prevention activities can include staff development and home-school events such as special assemblies with parents and carers. Schools should consider creative approaches which are relevant to the technologies their community use.
- Cyberbullying can be addressed within the curriculum, for example through citizenship and PSHE, and in relation to Spiritual, Moral, Social and Cultural development (SMSC). Other curriculum areas, including drama and computing, can also help bring cyberbullying issues to life.
- Make reporting incidents as easy as possible. Provide and publicise a range of reporting routes, including anonymous routes. Bystanders should be encouraged to take an active role in prevention by reporting any incident they witness.
- Digital literacy and e-safety are important for both pupils and staff. Staff should be confident to model the responsible and positive use of technology, and to respond to incidents of cyberbullying appropriately, including incidents linked to discrimination.
- Evaluate the effectiveness of cyberbullying prevention activities. Keep cyberbullying a live issue and celebrate your successes. Share effective practice with other schools and learning communities.

6.4 Responding to cyberbullying

To respond to cyberbullying:

- The school should act as soon as an incident has been reported or identified. This will include providing appropriate support for the person who has been cyberbullied; stopping the incident from spreading and assist in removing material from circulation; and working with the person who has carried out the bullying to ensure that it does not happen again.
- The person being bullied may have evidence of the activity and should be encouraged to keep this to assist any investigation. Cyberbullying can also be reported to the provider of the service where it has taken place.
- Provide information to staff and students on steps they can take to protect themselves online – for example, advise those targeted not to retaliate or reply; provide advice on blocking or removing

people from contact lists; and ask them to think carefully about what private information they may have in the public domain.

- 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 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.

6.5 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting (*please also see – Confiscation and Searching Policy*):

- Poses a risk to staff or pupils, 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 pupils and staff. If the search is not urgent, they will seek advice from the headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

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

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device had, 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 staff member in conjunction with the DSL/headteacher/other member of the senior leadership team 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 relation 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 practical. 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 pupil and/or the parent/carer refuses to delete the material themselves

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

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

Any searching of pupils 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 pupils' electronic devices will be dealt with through the school complaints procedure.

6.6 Artificial Intelligence (AI)

Artificial intelligence (AI) presents exciting opportunities to improve people's lives, including by making our public services better. If used safely, effectively and with the right infrastructure in place, AI can support every child and young person, regardless of their background, to achieve at school and college and develop the knowledge and skills they need for life. AI has the power to transform education by helping teachers focus on what they do best: teaching. This marks a shift in how we use technology to enhance lives and tap into the vast potential of AI in our classrooms.

Generative AI is one type of AI. It refers to technology that can be used to create new content based on large volumes of data that models have been trained on a variety of sources.

ChatGPT, Microsoft Copilot and Google Gemini are generative AI tools, built on large language models (LLMs). LLMs are a category of foundation models trained on large amounts of data, enabling them to understand and generate human-like content.

Tools such as ChatGPT, Microsoft Copilot and Google Gemini can:

- answer questions
- complete written tasks
- generate images, text or code
- respond to prompts in a human-like way

Other forms of generative AI can produce:

- audio
- simulations
- videos

AI is the defining technology of our age, and it is evolving at incredible speed. This technology has the potential to benefit the economy and meet societal challenges. This is not new, and we already use AI in everyday life for:

- email spam filtering
- media recommendation systems

- navigation apps
- online chatbots

Godstone Primary and Nursery School will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risk of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school. Staff are aware of the limitations and risks of this technology, to include inaccuracy, inappropriateness, bias, mis-contextual, intellectual property infringement, reliability and quality.

7. Acceptable use of the internet in school

All pupils, parents/carers, 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 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 use *Securly* to monitor the websites visited by pupils, staff, volunteers, governors and visitors (*where relevant*) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in *appendices 1 to 3*.

8. Pupils using mobile devices in school

Pupils in Year Six may bring personal mobile devices into school. These are to be turned off and handed in at the beginning of the school day, where they are then stored, and returned when children are dismissed at the end of the school day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (*see appendices 1 and 2*).

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.

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 SoftEgg.

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 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 pupils can recognise dangers and risks in online activity and can weigh up the risks
- 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 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 child protection and safeguarding policy.

12. Monitoring arrangements

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

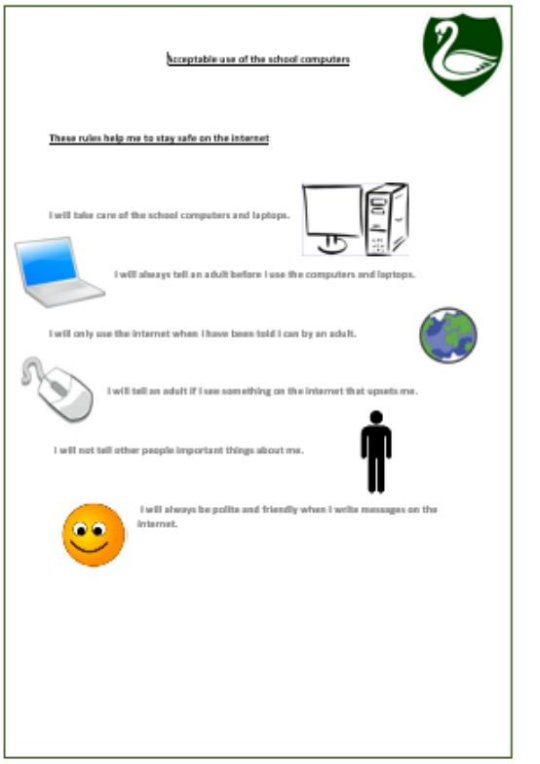
This policy will be reviewed every year by the computing lead, Emily Boden. At every review, the policy will be shared with the governing body. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and 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
- Computing policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Confiscation and Searching Policy

Appendix 1: EYFS and KS1 acceptable use agreement



Acceptable use of the school computers

These rules help me to stay safe on the internet

I will take care of the school computers and laptops.

I will always tell an adult before I use the computers and laptops.

I will only use the internet when I have been told I can by an adult.

I will tell an adult if I see something on the internet that upsets me.

I will not tell other people important things about me.

I will always be polite and friendly when I write messages on the internet.

Appendix 2: KS2 acceptable use agreement



Acceptable use of the school computers

These rules will help to keep everyone safe and help us to be fair to others.

- I will only use the school's computers and laptops for schoolwork and homework during lessons
- If attending Swans club, I will ask for permission to use games or websites.
- I will not tell anyone my logins and passwords
- I will only login to the school systems as myself
- I will only edit or delete my own files
- I am aware that some websites and social networks have age restrictions which mean that I should not go on them
- I will only visit internet sites that are appropriate for my age
- I will only communicate with people I know or that a responsible adult has approved
- I will only send polite and friendly messages
- I will not open an attachment, or download a file, unless I have been given permission by an adult
- I will not send or post photos or videos on the internet unless I have permission of an adult.
- I will not tell anyone my home address, phone number, give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- If I see anything I am unhappy with or I receive a message I do not like, I will show a trusted adult.

Appendix 3: Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
Name 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, unless specified as part of job role e.g. marketing the school via Facebook • 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 with teachers 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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
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 (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Acceptable user agreement (parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PARENTS/CARERS
Name of pupil:

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PARENTS/CARERS	
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 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, during 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 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 4: 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 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/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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?	