Godstone Primary & Nursery School

Online Safety Policy

REVIEW DATE: September 2021

REVIEWED BY: Acting Headteacher

NEXT REVIEW: September 2022

WRITTEN BY: Hayley Lancashire

Head Teacher: Candida Jarrott-Chase

Chair of Governors: Clare Thurman

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology

- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

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.

3. Roles and responsibilities

3.1 The governing body

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

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). 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

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 and deputies

Details of the school's DSL and deputies (DDSL) are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL and DDSL's take responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the headteacher, ICT technician and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 6) 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 governing board
- Ensuring that any online safety incidents are logged in the child protection folders and a brief comment logged (see appendix 6) 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
- Ensuring that parents/ carers get regular, timely online safety information

This list is not intended to be exhaustive.

3.4 The ICT technician

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, 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 (the school currently use the Surrey County Council recommended provider BTUnicorn as the ISP with a Smoothwall filtering system)
- 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 fortnightly basis and keeping a log of this
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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, including YouTube policy
- 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/DDSL's to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1, 2 and 3)

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

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 4).

4. Educating pupils about online safety

We believe that the key to developing safe and responsible behaviors online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings. Pupils will be taught about online safety as part of the curriculum:

Children in the early years use a range of technology to support their learning. The children are taught to use technology safely and not to share any personal information.

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.

From September 2020 **all** schools will have to teach relationships education and health education. Within this, there will be a focus on healthy, respectful relationships online.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters and communication via the newsletter. This policy will also be shared with parents.

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

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they

can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class, 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 (see section 11 for more detail).

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.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

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.

7 Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1- 4.

8 Pupils using mobile devices in school

Pupils in year 6 may bring personal mobile devices into school, but are not permitted to use them during the school day, including before and after school clubs. The mobile phone/electronic device need to be given in to the class teacher at the beginning of the school day and will be given back at the end of the school day.

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. Further information regarding mobile phone use can be found in the mobile phone policy.

9 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, as set out in appendix 4.

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

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

Work devices must be used solely for work activities.

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 policy on 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).

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 in the child protection folders, kept in a locked folder in the headteachers office. An incident report log can be found in appendix 5. This is used to keep a brief log of online safety issues.

This policy will be reviewed every year by the DDSL/Computing lead. At every review, the policy will be shared with the governing board.

13 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
- Mobile phone policy
- ICT and internet acceptable use policy

Appendix 1: Parent/Carer consent form and acceptable usage of the schools computers
Godstone Primary and Nursery School

Parent/Carer consent form and acceptable usage of the schools computers.
All pupils use computer facilities, including internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign agreements to show that the acceptable usage of school computers have been understood and agreed.

Parent / Carer name: ……

Pupil name:…… Year group ……

As the parent or legal guardian of the above pupil, I have read and understood the attached online safety rules and grant permission for my daughter or son to have access to use the internet, school email system, learning platform and other ICT facilities at school.

I know that my daughter or son has signed an online safety agreement form and that they have a copy of the school online safety rules. We have discussed this document and my daughter or son agrees to follow the online safety rules and to support the safe and responsible use of ICT at Godstone Primary and Nursery School.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files and the internet sites that they visit, and that if they have concerns about their online safety or e-behaviour they will contact me.

I understand the school is not liable for any damages arising from my child's use of the internet facilities.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent/Guardian signature:

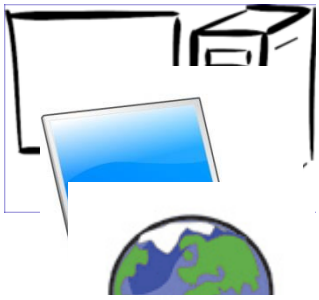
……Date**……**

Please complete, sign and return, via your child, to their class teacher
A copy of the EYFS/ KS1 and KS2 Acceptable Usage of the school computers are available to view on the school website.

Appendix 2: 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 3: 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 and Mathletics 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.

My name: . . . . . Date: . . . . . .

Appendix 4: acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I understand 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 5: Godstone Primary and Nursery School- You Tube Policy

Videos on the file-sharing website YouTube can be used to effectively support many areas of the curriculum. Additionally, there is a variety of music, song and dance performances appropriate for children. When these videos are used safely and appropriately, they can be an extremely beneficial resource for Class Teachers and Support Staff.

However, there are potential risks when working with YouTube that staff should be aware of. For example, despite a filter/flagging policy being in use on YouTube, inappropriate images, unsuitable written comments, or bad language can still all be accidentally revealed to the children. In order to prevent this from happening, the following precautions should be taken:

Finding suitable videos

- Searches, or first observations of a potential video, should not be carried out with any child in the class room.
- Before showing a video to the class, the video should be watched and listened to carefully by the Class Teacher or TA, who should look out for inappropriate content material along with any inappropriate comments that appear underneath the video.
- It is the class teacher's responsibility to make the final approval of a video.

Playing the video for the children

- Using the remote control, the Interactive Whiteboard should be frozen, stilled or muted (depending on the option available on your remote) prior to Full Screen mode being selected for the video. (This is so that no comments or any other videos can be seen by the children). When the video is ready, the Smartboard can be unfrozen and the video watched.
- Before the end of the video, pause it so 'recommended' videos, that might potentially contain inappropriate language, are not revealed.
- When the video is finished, the Smartboard should once again be frozen, stilled or muted (or even turned off) so that the video can be exited and the YouTube window closed safely.

Appendix 6: online safety incident report log

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