Online Safety Policy

Responsible Staff member: Hannah Cover

Governor Lead: Heather Archer

Reviewed: Spring 2021

Board approval date:

Policy Type: Non-Statutory, Safeguarding

Implementation date: Spring 2021

Publication: Guildford Grove Primary School

Review cycle: Annually

Next Review date: Spring 2022

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

Through our Online safety and Computing curriculum, we endeavour to promote our school aims which are as follows:

- To have a love of learning, so as to become lifelong learners
- To be taught to be responsible members of the community to improve their quality of life
- To be empowered to make informed choices, to keep them safe so that they fulfil their potential
- To have the highest aspirations for their future, to enhance their life chances.

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 Co-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 board

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

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

The governor who oversees online safety is Heather Archer as part of her safeguarding role.

Governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The Co-Headteachers

The Co-Headteachers are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and deputy DSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Supporting the Co-Headteachers in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Co-Headteachers, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are 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 the Co-Headteachers and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

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

- 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 weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents/ carers

Parents/carers are expected to:

- Notify a member of staff or the Co-Headteachers 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:

- 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 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the 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 class teaching and whole school assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents'/ carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/ carers via the school website.

Where appropriate, online safety will also be covered during parent consultation evenings.

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

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

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 safeguarding 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 and the subject will also be addressed in assemblies.

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school sends information on cyber-bullying to parents/ carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school 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 (where appropriate) and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

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

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils **are not allowed** to bring mobile devices into school.

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 3.

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 manager.

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 policies on behaviour and internet acceptable use policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. 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, safeguarding memos 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. An incident report log can be found in appendix 5.

This policy will be reviewed every two years by the online safety 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

Appendix 1: Child acceptable use agreement (pupils and parents/carers)

Guildford Grove Primary School
ICT Code of Conduct

- I will only use ICT as part of my education and I will only access information that is useful to me in my studies.
- I will only communicate using the internet after I have been given permission to do so by my teacher.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give personal information such as my address, telephone number, or the name and location of my school without my parents' or teachers' permission.
- I will not tell other people my ICT passwords.
- I will tell my teacher or my parents/ carers right away if I come across any information that makes me feel uncomfortable.
- I will not deliberately look for, share or send anything that could be unpleasant or nasty.
- I will not respond to any messages that are mean or in anyway make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my teacher or my parents right away.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/carer can be contacted if a member of school staff is concerned about my online safety.

Signed

Name of pupil (printed) _____ Class _____

Signature of pupil _____

I have read the code of conduct with my child and we understand that if any of these rules are broken my child will not be able to use the computers at school for an appropriate amount of time.

Name of parent/carer (printed) _____

Signature of parent/carer _____

Appendix 2: Parent/ carer acceptable use agreement (pupils and parents/carers)

Guildford Grove Primary School

Parents' ICT Code of Conduct

This code of conduct is designed to ensure that all parents are aware of their responsibilities when using any form of ICT. All parents and children from schools other than Guildford Grove are expected to sign this code of conduct and adhere at all times to its contents (Guildford Grove pupils will have signed a separate Code of Conduct). Further information can be sought from the school Online Safety Policy and any concerns or clarification should be discussed with the Online Safety Co-ordinator.

- I appreciate that ICT includes a wide range of systems including computers, the internet, mobile phones, PDA's, digital cameras, e-mail and social networking.

- Personal ICT equipment may only be used in the school when agreed in advance with the Online Safety Coordinator i.e. Use of personal mobile phones on a school trip.

- I will only use the school's ICT for uses deemed 'reasonable' by the Head or Governing Body.
- I understand that it is a criminal offence under The Computer Misuse Act 1990 (sections 1–3) to use the school's ICT system for a purpose not permitted by its owner.
- I will report any incidents of concern regarding children's safety to the Online Safety Co-ordinator, the Children Protection Officer or Co-Headteachers.
- I will not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out on the ICT equipment assigned to me for the duration of my session.
- Images of children and/ or staff will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Co-Headteachers.
- I will respect copyright and intellectual property rights.
- I understand that all Internet usage and network usage can be logged.
- I will support and promote the school's Online Safety Policy and help children and other adults to be safe and responsible in their use of ICT and related technologies.

The school reserves the right to revoke access to the ICT systems where it is believed that unauthorised use may be taking place.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …… Date ……

Full Name ……..(printed)

Appendix 3: Staff, governor and visitor agreement

Guildford Grove Primary School

Staff, Governor and Visitor ICT Code of Conduct

ICT is an expected part of our daily working life in school. This code of conduct is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this code of conduct and adhere at all times to its contents. Further information can be sought from the school Online Safety Policy and any concerns or clarification should be discussed with the Online Safety Co-ordinator.

- I appreciate that ICT includes a wide range of systems including computers, the internet, mobile phones, PDA's, digital cameras, e-mail and social networking.
- Personal ICT equipment may only be used for school business when agreed in advance with the Online Safety Coordinator i.e. Use of personal mobile phones on a school/centre trip.
- I will only use the school's ICT for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I understand that it is a criminal offence under The Computer Misuse Act 1990 (sections 1–3) to use the school's ICT system for a purpose not permitted by its owner.
- I will report any incidents of concern regarding children's safety to the Online Safety Co-ordinator, the Children Protection Officer or Co-Headteachers.
- I will ensure that sensitive data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Sensitive data can only be taken out of school or accessed remotely if it is listed in the Data Security section of the school Online Safety Policy or when authorised by the Co-Headteachers, Online Safety Co-ordinator, Information Asset Owners or Governing Body.
- I will not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will only use the approved email system for any school business.
- I will ensure that all electronic communications and online activities are compatible with my professional role.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Co-Headteachers.
- I will respect copyright and intellectual property rights.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I will support and promote the school's Online Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

The school reserves the right to revoke access to the ICT systems where it is believed that unauthorised use may be taking place.

Appendix 3 continues:

Staff ICT Code of Conduct /Consent of Images
(to be kept in Personnel file)

Images at work:

- I consent/do not consent* for the school to use images of me at work for professional purposes only.** delete as appropriate*

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …….…… Date ……

Full Name ……..(printed)

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?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log