Goring C E Primary School

Faith, Love and Learning

Online Safety Policy

Date adopted by Governing Body: Spring Term 2024
Date of next review: Spring Term 2025

To be read in conjunction with Acceptable Use Policy

Headteacher - Mrs Clare Jee

Mission – what is our reason for being?

- **To educate**
- **To nurture**
- **To serve the community**
- **To develop children's faith and spirituality**
- **To be inclusive**
- **To improve life outcomes**
- **To develop children's life and learning skills**
- **To develop morals and principles**

Our School Values:

- ✓ **Love**
- ✓ **Faith**
- ✓ **Self-worth**
- ✓ **Respect**
- ✓ **Aspiration**
- ✓ **Equality**
- ✓ **Fun**

Our School Vision for 2025:

To be a Church of England Primary School community that:

- **Nurtures each individual as a whole person, enabling them to achieve their God given potential and make outstanding progress**
- **Demonstrates love and respect for all of God's creation**
- **Provides an exciting, broad and ambitious curriculum that equips learners for the future**

Contents

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**

1. 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 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.

2. 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 board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Leads (DSLs).

All governors will:

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

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 leads

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

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

- **Supporting the staff to understand this policy and that it is being implemented consistently throughout the school**
- **Working with the Headteacher, ICT manager, computing lead and other staff, as necessary, to address any online safety issues or incidents**

- **Ensuring that any online safety incidents are logged 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 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 Headteacher and/or governing board**

3.4 The ICT Support assistant

The ICT support assistant 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 continuous 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 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**

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, and ensuring that pupils follow the school's terms on acceptable use**
- **Working with the DSLs 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**

3.6 Parents

Parents are expected to:

- **Notify a member of staff or the Headteacher of any concerns or queries regarding online safety**
- **Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet**

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

- **What are the issues? - UK Safer Internet Centre**
- Common Sense Media: Age-Based Media Reviews for Families | Common Sense Media
- **Parent factsheet - Childnet International**
- **Hot topics - Childnet International**
- Home (lgfl.net)

- Home - Safer Internet Day
- Keeping children safe online | NSPCC
- Parents and carers | CEOP Education (thinkuknow.co.uk)

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.

3. Educating pupils about online safety

At Goring, pupils will be taught about online safety and digital citizenship as part of the curriculum:

In Key Stage 1, pupils will be taught to:

- **use technology purposefully to create, organise, store, manipulate and retrieve digital content**
- **recognise common uses of information technology beyond school**
- **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**

In Key Stage 2 will be taught to:

- **understand computer networks, including the internet; how they can provide multiple services, such as the World Wide Web, and the opportunities they offer for communication and collaboration**
- **use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content**
- **use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact**

By the end of Year 6, 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 taught in PSHE and other subjects where relevant. See the National Curriculum computing programmes of study for further detail.

4. Educating parents about online safety

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

There will be an annual parent online safety and digital citizenship Workshop / Talk.

Online safety will also be covered during Parent Information evenings.

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

Concerns or queries about this policy can be raised with any member of SLT 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, such as during online gaming, 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.

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) will receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSLs 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.

Where school are made aware of underage use of social media platforms, the school will report this to the relevant platforms and will inform parents.

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 and the school's COVID-19 risk assessment.

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

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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.

8. Remote Learning

All staff and pupils must only use Microsoft Teams and emailing (using school email addresses only) for any online communication. Staff and pupils should not engage, or make any attempt to engage, with communication via any social media platforms.

The Senior Leadership Team and Computing Lead (and other agreed and directed staff) may use our school Twitter account to communicate and share with parents outside of school. Staff must adhere to the Acceptable Use Policy at all times when using this platform, and must only use our school Twitter account for educational or community engagement purposes.

All staff and pupils using video communication must:

- Wear suitable clothing
- Be situated in a 'public' living area within the home, with an appropriate background
- Not allow people outside of our school community to be visible on camera
- Use appropriate language
- Maintain the standard of behaviour expected in school
- Not record, store, or distribute any video content without permission
- Always remain aware that they are visible
- Use Microsoft Teams and other computer software appropriately and for learning purposes only

Pupils not using devices or software as intended will be disciplined in line with our Behaviour Policy.

During periods of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online
- Ensure parents are aware of what their children are being asked to do
- Encourage them to set age-appropriate parental controls on devices, and internet filters to block malicious websites

The school will ensure that any school-owned devices which are loaned out to children are secure, and have appropriate safety software installed, such as anti-virus and filtering software.

9. Pupils using mobile devices in school

Pupils in Year 5 and 6 may bring mobile devices into school with parental consent. This is ONLY for use while travelling to/from school, and class teachers will keep all devices together securely, away from children's access during the school day.

Pupils' devices must be switched off before entering the school site, and must not be switched on until they are off the school site at the end of the 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.

10. 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)**
- **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 filtering software**
- **Keeping operating systems up to date – always install 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.

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 the ICT Manager.

11. 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 behaviour policy and acceptable use policy. 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.

12. 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 DSLs 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.

13. Monitoring arrangements

Behaviour and safeguarding issues related to online safety will be reported using our existing safeguarding reporting system: CPOMS.

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

14. Links with other policies

This online safety policy is linked to our:

- **Child protection and safeguarding policy**
- **Behaviour policy**
- **Staff disciplinary procedures**
- **Data protection policy and privacy notices**
- **Complaints procedure**
- **ICT and internet acceptable use policy**