# Grendon CE Primary School
# Online Safety Policy

## 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 document, Keeping Children Safe in Education (2023), and its guidance for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Head Teachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Meeting digital and technology standards in schools and colleges

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 Head Teacher 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 understand this policy
- adhere to the terms on acceptable use of the school's ICT systems and the Internet (Appendix 2)

### 3.2 The Head Teacher

The Head Teacher 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 Deputy

Details of the school's DSL and DDSL are set out in our Safeguarding and Child Protection 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 staff to address any online safety issues or incidents
- ensuring that any online safety incidents are logged (see appendix 3) 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 and discipline 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

This list is not intended to be exhaustive.

### 3.4 The ICT manager

In order to keep children safe when using school IT equipment, we commission a specialist ICT company, EasiPC, to install and manage the appropriate level of filtering. 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 fortnightly basis
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- being mindful that "over-blocking" can lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding and mitigate against this by teaching a comprehensive programme of Internet Safety.

### 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 2), and ensuring that pupils follow the school's terms on acceptable use (Appendix 1)
- working with the DSL and DDSL to ensure that any online safety incidents are logged (see Appendix 3) 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 and discipline policy

### 3.6 Parents

Parents are expected to:

- monitor their child's safe and appropriate internet use (including Teams) outside of school
- ensure that appropriate safeguarding controls are in place on their home internet and personal devices
- supervise their child's internet usage, including appropriate time limits and curfews
- notify a member of staff or the Head Teacher of any concerns or queries
- ensure their child has fully understood the acceptable use rules (Appendix 1)

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 2).

## 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

Aspects of online safety will taught through Relationships and Health Education (see RHE Policy).

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.

## 5. Educating parents about online safety

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

Online safety may also be covered during dedicated parent information sessions.

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

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

## 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.

### 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.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

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 12 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and discipline 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.

This specific power extends to the school's learning platform, Microsoft Teams, which is regularly monitored by school staff.

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

Through their attendance/involvement in school, pupils, parents, staff, volunteers and governors are automatically expected to agree and adhere to the school's expectations around online safety (Appendices 1 and 2).

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

## 8. Learning Platform: Microsoft Teams

As part of the school's Remote Learning Strategy, the school uses Microsoft Teams as its preferred Learning Platform. The school's expectation is that pupils will engage responsibly and safely with technology as part of their curriculum provision and that they will engage.

Pupils must be aware that the school has a duty to monitor the use of its Learning Platform and that anything pupils share via any part of their school Microsoft Teams account can be viewed, at any time, by school staff as part of their monitoring role. To ensure that the school's Learning Platform is a safe and controlled environment, its contents are visible at all times to school staff and it should not be regarded as a private platform.

## 9. Pupils using mobile devices in school

Pupils are not permitted to use mobile devices in school. If a pupil were to bring a mobile device into school then it should be kept in a secure place in the classroom and returned to the child at the end of the school day.

## 10. 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 2.

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.

### 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 & Discipline 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 Safe Behaviour Policy. 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. An incident of misuse outside of school will only be investigated where the DSL believes that it constitutes a safeguarding issue (see Child Protection & Safeguarding Policy).

### 12. Training

The DSL and DDSL will undertake child protection and safeguarding training, which will include online safety, every year. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Staff and governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding updates.

Volunteers will receive appropriate training and updates, if applicable.

### 13. Monitoring arrangements

The DSL and DDSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 3.

This policy will be reviewed annually by the DSL and DDSL. At every review, the policy will be shared with the governing body.

### 14. Links with other policies

This online safety policy is linked to these policies:

- Child Protection & Safeguarding Policy
- Behaviour and Discipline Policy
- Anti-Bullying
- GDPR
- Safe Behaviour
- Complaints Procedure
- Sex and Relationship Educations
- Global Curriculum Handbook
- Relationships and Health Education
- School Protocol for Volunteers
- Safeguarding Pupils: Parent Guide
- Safeguarding Pupils: Visitor Guide
- Off-site Visits

**Appendix 1**

## Pupils’ Acceptable Use Rules

- I will ask a teacher or adult for permission to use the Internet
- I will only use websites that a teacher or adult has told me or allowed me to use
- I will tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don’t know
    - I find anything that may upset or harm me or my friends
- I will use school computers for school work only
- I will be kind to others and not upset or be rude to them
- I will look after the school ICT equipment and tell a teacher straight away if something is broken
- I will never share my password with anyone, including my friends
- I will tell a member of staff immediately if I find any material that is inappropriate or upsets me
- I will never give my personal information to anyone without the permission of my teacher or parent
- I will upload my school work onto the school Learning Platform
- I will check with my teacher before I print anything
- I will log off/shut down a computer when I have finished using it
- I understand that the school will monitor my school Teams account along with the websites I visit
- I will not access any inappropriate websites including social networking, chat rooms and gaming sites
- I will not open any attachments in emails, or follow links in emails, without first checking with a teacher
- I will not use any inappropriate language or images when communicating online, including in emails
- I will not attempt to log into an account that doesn’t belong to me

## Parents’ Agreement

- I agree that my child can use the school’s internet when supervised by a member of school staff
- I agree to the conditions set out above and will ensure that my child understands them
- I will enforce the Pupils’ Acceptable Use rules outside of school

**Appendix 2:**

**Staff, Governors and Volunteers Acceptable Use Rules**

**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
- 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
- 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 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.

**Appendix 3: 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** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |