Grimoldby Primary School

Online Safety Policy

(including Social Networking and Acceptable Use)

Date Approved: May 2026

Date for Review: May 2028
Online Safety Leader: Mrs B Taylor
Named Governor for Online Safety: Mrs D Berry

Online Safety

Aims

To ensure that the requirement to empower the whole school community with the knowledge to stay safe and as risk-free as possible is met.

To ensure risks are identified, assessed and lessened (where possible) in order to reduce any foreseeable harm to the pupils or liability of the school. This policy sits in conjunction with our Anti-Bullying Policy.

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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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

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
- Meeting digital and technology standards
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health 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 sits in conjunction with our *Monitoring & Filtering* document

Role of the governing body

The governing body is accountable for ensuring that our school has effective policies and procedures in place that teaches pupils how to keep themselves and others safe, including online, and, as such, they will:

- Review this policy regularly and in response to any Online Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, and ensure that any Online Safety issues are dealt with appropriately;
- Appoint one governor to have overall responsibility for the governance of Online Safety at the school who will keep up to date with emerging risks and threats through technology use and receive regular updates from the Headteacher in regard to training, identified risks and any incidents.
- 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.
- Ensure all staff receive regular online safety updates, as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- Make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness.

Role of the Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for Online Safety within our school. The day-to-day management of this will be delegated to the named member of staff above. The Headteacher will ensure that:

- Online Safety training throughout the school is planned, up to date and appropriate to the recipient;
- Staff understand this policy, and that it is being implemented consistently throughout the school;
- All Online Safety incidents are dealt with promptly and appropriately.

Role of the Online Safety Leader

The Online Safety Leader will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themself with the latest research and available resources for school and home use;
- Review this policy regularly and bring any matters to the attention of the Headteacher;
- Advise the Headteacher and governing body on all Online Safety matters;
- Engage with parents and the school community on Online Safety matters at school and/or at home;

- Liaise with the local authority, IT technical support and other agencies as required;
- Retain responsibility for the Online Safety risk assessment;
- Ensure any technical Online Safety measures in school (e.g. Internet monitoring and filtering software) are fit for purpose through liaison with the local authority and/or IT technical support.

Role of the IT technical support staff

Technical support staff are responsible for ensuring that:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices;
- Operating system updates are regularly monitored, and devices updated as appropriate;
- Any Online Safety technical solutions such as Internet filtering are operating correctly;
- Filtering levels are applied appropriately according to the user (staff and pupils);
- Passwords are applied correctly to all users regardless of age;
- The IT System Administrator password is changed on a regular basis.

Role of all other staff and volunteers

Staff are to ensure that:

- All details within this policy are understood and implemented consistently. If anything is not understood it should be brought to the attention of the Headteacher;
- **They work with the DSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy;**
- **Any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy;**
- **They respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintain an attitude of 'it could happen here.'**

Role of Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Parents/carers can seek further guidance on keeping children safe online from resources on the school website and through Childnet.

Educating pupils about online safety

Pupils will be taught about online safety as part of the Computing curriculum. The safe use of social media and the internet will also be covered in other subjects where relevant, including age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

In Key Stage (KS) 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 (KS) 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

- Be discerning in evaluating digital content

By the end of primary school, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

Risk assessment of potential issues/dangers

The Online Safety Leader will ensure that the risk assessment is kept up-to-date in line with technological developments within the school (located at the end of this policy). The risk assessment will be shared with all staff members and the school's IT technical support provider.

In the event of staff/pupils accidentally accessing online material that they deem to be inappropriate/offensive, it will be reported to the Online Safety Leader or, in their absence, to the Headteacher.

Protection against extremism/radicalisation

Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence use the Internet as a means of either inciting violence against specific groups or providing information on carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

- Appropriate filtering is in place and will be reviewed whenever there is an incident of pupils accessing websites advocating extremism;
- The Online Safety Leader will record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school or its pupils;
- A referral will be made to the police whereby a pupil is deeply involved in the extremist narrative and there is evidence that their parents are involved in advocating extremist violence.

Cyber-bullying

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy).

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 encourage them 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, finding 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.

The school also sends information/leaflets on cyber-bullying to parents/carers and signposts them to the Online Safety area on the school website so 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 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.

Child on child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school responds to all concerns regarding online child on child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Supporting pupils' mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

Social Networking

1 Staff and governors using social networking websites and/or apps

1.1 Staff are within their rights to use social networking websites and we are not, nor would not want to be, in a position to prevent staff from using them. However, we do ask that staff adhere to the following aspects of our policy:

1.2 Under no circumstances should pupils or ex-pupils under the age of 13 be befriended on a social networking website. If a child requests the befriending of a staff member, their parents should be informed.

1.3 In the event that a parent makes contact with a staff member through a social networking website, the staff member must use extreme caution and it is recommended that they provide their school email address as a point of contact for professional purposes. In the event of communicating with a parent or adult associated with a child who attends the school, no comments should be made about pupils, staff or parents.

1.4 Any statements or status remarks published on personal social media, in any capacity, should not contain any comments about the school, staff, parents or pupils – unless it is a direct share of a post from the school's own social media account.

1.5 All views expressed by staff members on social networking websites are their personal views and are in no way endorsed, nor supported, by the school. Staff should always assume that anything posted on social media would be attributed to them as a professional.

1.6 School employees and volunteers must not identify themselves as associated with the school in any way, unless expressly authorised by the Headteacher. Authority to use official school social media will be given to individual members of staff by the Headteacher.

2 Pupils using/accessing social networking websites and/or apps

2.1 Under no circumstances should a child access social networking websites in school unless it is for a purpose instigated by the child's teacher. The school network system prohibits pupils from accessing these websites but the bypassing of the system or accessing through a mobile phone is strictly prohibited.

2.2 If any reports are received of pupils making inappropriate comments about staff or other pupils, hard copies will be obtained and the child will be reported immediately (to the website host) to have their account terminated. The parents/carers of the child will also be notified, and this could result in further action. If the comment is about a member of staff a referral may be made to the county's legal services.

3 Parents using social networking websites and/or apps

3.1 If hard copies of inappropriate comments about members of staff, pupils within the school or school decisions are received, the matter may be referred to the county's legal services and subsequent action will follow.

3.2 School visits: parents must not, under any circumstances, access social networking accounts whilst assisting staff members. They must also ensure that they do not take photographs/videos on a personal device. If there is evidence to prove that this has happened, then the parent will no longer be used as a helper on subsequent visits. If this is considered a GDPR breach, it will be reported in accordance with our GDPR policy.

Artificial Intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Grimoldby Primary School recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Grimoldby Primary School will treat any use of AI to bully pupils very seriously, in line with our Behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Acceptable Use of the internet in school

1 Aim

1.1 The aim of this section of the policy is to ensure that pupils will benefit from learning opportunities offered by the school's Internet and technological resources in a safe and effective manner.

2 General

2.1 Pupils will be supervised by an adult whilst using the Internet. Online Safety is taught as part of our Computing curriculum.

2.2 Filtering systems (two-level) are used by our Internet Service Provider in order to minimise the risk of exposure to inappropriate material.

2.3 Downloading of non-approved software is prohibited (approval to be sought by Online Safety Leader or Headteacher).

2.4 Virus protection is present and maintained on all relevant devices.

2.5 The use of personal portable storage media (USB memory sticks/hard drives) for pupils requires the permission and supervision of a teacher.

2.6 Staff will require permission from the Headteacher to use portable storage media (USB memory sticks, discs, SD cards, etc) on any school device. Any such device containing sensitive or pupil data must be encrypted in order to prevent GDPR breaches.

2.7 Staff should keep personal passwords private. Under no circumstances should a personal password be shared with a staff member, pupil or IT technical support staff. If staff feel that a password has been compromised, they should report this to the Headteacher or Online Safety Leader immediately.

2.8 Passwords to whole-school resources can be shared so long as password access does not lead to any pupil information other than name and year group.

3 World Wide Web

3.1 School staff and pupils will not intentionally attempt to access material deemed inappropriate or material that is blocked by filtering systems.

3.2 Pupils will not copy information from other sources without acknowledging and citing the original source (copyright infringement).

3.3 Pupils will never disclose or publicise personal information.

4 Email/Microsoft Teams

4.1 School staff and pupils will only use approved email and Microsoft Teams accounts whist on site.

4.2 School staff and pupils will not send material that is illegal, obscene, defamatory or material that is intended to annoy or intimidate another person.

4.3 Pupils will never arrange a face-to-face meeting with someone they know only through the Internet.

4.4 All communication will be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

5 Personal devices

5.1 Pupils may only bring personal devices into school with permission from their teacher.

5.2 Pupils' personal devices will not be allowed to access Internet in school unless under exceptional circumstances (agreed by the Online Safety Leader or Headteacher).

6 Portable devices/tablets

6.1 School teachers will be provided with an Apple iPad for use within their class and at home for a range of purposes.

6.2 Apple iPads will be password locked with all data set to be erased following 10 unsuccessful password attempts.

6.3 Apple iPads will not be used by any friends or family members outside of school.

6.4 Pupils may use staff Apple iPads but only when directly supervised.

6.5 All apps (paid and unpaid) will be managed via the Apple Volume Purchase Program (VPP) by the Online Safety Leader or the School Business Manager.

6.7 The pupil bank of iPads will only be used under adult supervision.

7 Mobile phones/smart devices

7.1 School staff, volunteers, parents and contractors are allowed to bring in personal mobile phones/smart devices for their own use. Staff, volunteers, parents and contractors should use their personal mobile phones/smart devices with caution. The responsible use of personal mobile phones and devices is based on an agreement of trust that; **During times when children are on the school premises, phones must be kept *on silent and out of sight.*** Staff, volunteers, parents and contractors may only make and receive calls out of school hours or in an emergency in the staff room.

7.2 Users bringing personal mobile phones/smart devices into school must ensure that there is no inappropriate or illegal content on the device – even if this is not immediately accessible or visible.

7.3 Staff, volunteers, parents and contractors will not use mobile devices to take images or videos of pupils, staff or any area of the school environment.

7.4 If school staff have a family emergency or similar and are required to keep their personal mobile phone to hand, prior permission must be sought from the Headteacher.

7.5 Staff, volunteers, parents and contractors will not access the WiFi system using personal mobile devices, unless permission has been given by the Headteacher.

7.6 **Children** are permitted to have a mobile phone in school if they are in KS2 and walk to and from school unaccompanied. All mobile phones belonging to children must be switched off and left in a locked cabinet in the staff room. They are not to be used on the school premises.

8 Examining electronic devices

8.1 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:

- 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

8.2 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 one of the school's DSLs
- 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

8.3 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 has, 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 Headteacher 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.

How the school will respond to issues of misuse

Where a pupil misuses the school's internet, we will follow the procedures set out in our behaviour 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 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Online safety training for staff

As part of our Safeguarding training pathway, all staff undertake training in online safety. However, in addition to this, all staff receive annual face-to-face online safety training from an online safety advisor.

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, threatening, 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

Risk Assessment

Risk	Likelihood	Impact	Score*	Actions
Access to inappropriate content (staff)	1	3	3	Appropriate Internet filtering is in place.
Access to inappropriate content (pupils)	2	3	6	Appropriate Internet filtering is in place, set to a higher level than staff access. This is a two-level system: one at router level, the other via SENSO Cloud.
Access to staff files, documentation or filtering level	1	2	2	Policy states that pupils will only use staff iPads when under direct supervision. Staff PCs to be locked when not in direct use/view.
Misuse of copyright material (staff/pupils)	2	2	4	Pupils are taught about copyright as part of the Online Safety element of the Computing curriculum. Staff aware of copyright guidelines.
Loss/theft of personal pupil data	1	3	3	Encryption and security measures to be in place on all IT equipment as necessary.
Misuse/inappropriate activity on pupil iPads by pupils	2	3	6	iPads set to pupil level of filtering with certain features/functions disabled and monitored via SENSO Cloud. Filtering at router level also in place. Pupils to be supervised when using iPads.
Theft of iPads	2	1	2	iPads locked in secure cabinet and updated regularly with latest iOS. iPads protected with passcodes and GPS location discoverable via built-in software.
Theft of off-site school property (eg: laptops, iPads)	2	3	6	Any off-site device to be encrypted and kept as safe as possible. Staff to ensure necessary due diligence.

*

This is the product of the likelihood and the impact, and is categorised as below:

1 – 3 = low risk

4 – 6 = medium risk

7 – 9 = high risk