

E-Safety Policy



Approved by: FGB

Date:

Last reviewed on: April 2026

Next review due by: May 2028

Document & Version Control			
Statutory for Website	No	Review Cycle	2 Years

Revision Date	Version No.	Summary of Change	Changes made by	Approved by	Date approved
April 2026	1	New document		FGB	

Contents

Purpose of Study and Aims	2
Our approach to the teaching of e-safety.....	3
In Key Stage 1, pupils will be taught to:	4
In Key Stage 2, pupils will be taught to:	4
By the end of Year 6, pupils will know:	4
Use of digital and video images - photographic, video	5
Pupils using mobile devices in school	5
Staff using work devices outside school	5
Communication technologies	6
The role of Governors	6
The role of the Headteacher / Senior Leaders	6
The role of Technical staff	7
The role of Teachers / Support staff.....	7
The role of Designated Safeguarding Lead (DSL)	7
The role of Pupils	8
The Role of Parents / Carers.....	8
The role of all staff and volunteers	9
Resourcing / CPD.....	9
Reporting to Parents and Carers	9
Monitoring agreements	9
Links to other Policies	10

Purpose of Study and Aims

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies including Artificial Intelligence (AI) are powerful tools, which open up new opportunities for everyone. Electronic communication helps

teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The purpose of a school e-safety policy is to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents and carers, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the offline world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. Behaviour, Anti-bullying and Child Protection and Social Media policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Gastrells Primary School will demonstrate that it has provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. Our e-safety policy explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Our approach to the teaching of e-safety

Regulation and technical solutions play a critical role in e-safety. Additionally, Gastrells Primary School recognises the importance of educating pupils to take a responsible approach to their use of technology.

E-safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of Computing / PHSE / other lessons and will be regularly revisited – this will cover both the use of computing and new technologies in school and outside school.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and teaching times.
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line.
- Pupils will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff will act as good role models in their use of ICT, the internet and mobile devices

In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Where students / pupils are allowed to freely search the internet, e.g. using search engines, staff must be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the relevant person can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

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.

In Key Stage 2, pupils 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 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 covered in other subjects where relevant.

Use of digital and video images- photographic, video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Staff are allowed to take digital / video images to support educational aims, but must follow school policies (see Social Media policy) concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, Twitter, Class page, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published online.

Pupils using mobile devices in school

All pupils are discouraged from bringing mobile devices into school however, if they are not brought to, or collected by a parent or other responsible adult, they may do so by agreement with the school. This may be because they walk to or from school on their own.

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 term of acceptable use, as set out in the acceptable use agreement for staff, governors, volunteers or visitors.

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, including in public spaces.

If staff have any concerns over the security of their device, they must seek advice from the school's IT provider.

Communication technologies

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report to the Head Teacher the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website, and only official email addresses should be used to identify members of staff.

The role of Governors

Governors have overall responsibility for the approval of this E-Safety Policy and for reviewing its effectiveness.

The governing board will coordinate regular meetings with appropriate staff to discuss online safety, receiving regular information about e-safety incidents and monitor online safety logs as provided by the designated safeguarding lead.

All governors will ensure that they have read and understood this policy, and will agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

The role of the Headteacher / Senior Leaders

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

The Headteacher / Senior Leaders are responsible for ensuring that staff receive suitable CPD to enable them to carry out their e-safety roles.

The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The role of Technical staff

The school has an external ICT service provided by Focus Networks. The school ensures that the service provider carries out all the e-safety measures that would otherwise be the responsibility of the school's technical staff.

Focus Networks will ensure the following -

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the e-safety technical requirements.
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- FN is informed of issues relating to the filtering applied.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher / Senior Leader / Class teacher) for investigation, action or sanction.
- That monitoring software / systems are implemented and updated as agreed in school policies.

The role of Teachers / Support staff

Teachers / support staff will ensure that -

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP).
- They report any suspected misuse or problem to the Head teacher / Senior Leaders / Class teachers for investigation, action or sanction.
- Digital communications should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school e-safety and acceptable use policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

The role of Designated Safeguarding Lead (DSL)

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 to address any online safety issues or incidents.
- Ensuring that online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.

The DSL should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

The role of Pupils

All pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. At KS1 it would be expected that parents / carers would sign on behalf of the pupils.

All pupils –

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Need to understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school.

The Role of Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore keep parents and carers informed of these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy
- Accessing the school website records in accordance with the relevant school Acceptable Use Policy.
- Notifying a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Ensuring their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

Parents and carers can seek further guidance on keeping children safe online from the following organisations and websites. We will regularly inform parents and carers of websites they can use for this, including:

- What are the issues? - [UK Safer Internet Centre](#)
- Hot topics - [Childnet International](#)
- Parent factsheet - [Childnet International](#)

The role of all staff and volunteers

All 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.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Locking computers / devices at times such as breaks to ensure there is no leaking of data.
- Ensuring that email and computer passwords are changed annually.

Resourcing / CPD

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be provided as follows -

- 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, staff meetings).
- The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years.
- 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.

Reporting to Parents and Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of children's on-line experiences. Parents and carers often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The school will provide information and awareness to parents and carers through:

- Letters, newsletters, school website, Class Dojo, Twitter
- Parents evenings

Monitoring agreements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every two years. At every review, the policy will be shared with the governing board.

Links to other Policies

Safeguarding

Acceptable Use

Social Media

Data Protection (GDPR)

Mobile Phones & Electronic Devices