Gunthorpe Church of England Primary School

E-Safety and Acceptable Use Policy

Responsibility of:	**Governing Body**
Approved on:	**Feb 2025**
Review Date:	**Feb 2028**

This E Safety and Acceptable Use Policy outlines the commitment of Gunthorpe C of E to safeguard members of our school community online in accordance with statutory guidance and best practice.

Introduction

Computing is an integral part of the national curriculum and a key skill for everyday life. Computers, tablets, programmable robots, digital and video cameras are a few of the tools that can be used to acquire, organise, store, manipulate, interpret, communicate and present information. We recognise that pupils are entitled to quality hardware and software and a structured and progressive approach to the learning of the skills needed to enable them to use them effectively.

Computing sits within the STEAM curriculum team at Gunthorpe and our intent is as follows:

We aim to ensure opportunities for children to engage in a range of practical, investigative and problem solving activities where there are opportunities to use their creativity, develop technical and problem solving skills in a variety of contexts reflecting the digital and complex world around them. We encourage children to immerse themselves in risk taking, innovative, imaginative thinking, be active participants, adopting resilient approaches to explore solutions and communicate outcomes. By allowing children to explore their expressive side and develop their ideas we hoping to engage, inspire and equip them with the skills they need to experiment, invent and create.

Pupils will be taught about online safety as part of the curriculum in line with National Curriculum computing programmes of study and guidance on relationships education, relationships and sex education (RSE) and health education.

Aims

Aspire is committed to ensuring the safety of students in the digital world. Our academies have implemented comprehensive online safety measures and educate students about the potential risks of online activity

Gunthorpe aims to:

Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

Identify and support groups of pupils that are potentially at greater risk of harm online than others

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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, fake news, 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 them 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 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.

Roles and Responsibilities

To ensure the online safeguarding of members of our school community, it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the E Safety Policy, for reviewing the effectiveness of it and ensuring that our school has other effective policies and procedures in place. They will:

- Review the policy every 2 years and in response to any National policy updates and e-safety incidents to ensure the policy is up to date and covers all aspects of technology use within school.
- Appoint a Governor to have online safety responsibility. Keeping up to date with emerging risks/threats through technology use and receive regular updates from the Head in regards to training, identifying risks and any incidents that happen.
- The governing body will also support the school in encouraging parents and carers and the wider community to become engaged in online safety activities.

Headteacher and Senior leaders

Reporting to the governing body, the Headteacher has overall responsibility for e-safety within our school. E-Safety training throughout the school will be planned in by Senior leaders. It will be up to date and appropriate to the recipient, ie pupils, staff, SLT, governing body and parents.

All e-safety incidents will be dealt with promptly and appropriately by the Headteacher and the assistant Head. They have the responsibility to be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. The headteacher will ensure that there is a system in place to allow for monitoring (RM Safetynet) and will run regular monitoring reports. In addition, they will ensure that any technical e-safety measures in school (eg filtering software) are fit for purpose through liaison with technical support (RM).

Lead Teacher for Computing and E-safety (STEAM TEAM)

The team will ensure staff have an up-to-date awareness of e-safety matters, working closely on a day-to-day basis with the Designated Safeguarding Lead(s) (DSLs). They will promote an awareness of and commitment to online safety education and raise awareness across the school and beyond.

In addition, they will update school computing curriculum content, as appropriate and monitor curriculum delivery and outcomes, ensuring that the online safety curriculum is planned, progressive and embedded.This will be provided through the iLearn2 computing scheme of work, supported by Coram Life Education's schemes of work (PSHE) and national initiatives such as Safer Internet Day and Anti Bullying week.

Designated Safeguarding Lead(s):

The DfE guidance 'Keeping Children Safe in Education' (2024) states: "The DSL has overall responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place".

The Designated Safeguarding Lead(s) should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- Sharing of personal data (see Data Protection Policy)
- Access to illegal/ inappropriate materials
- Inappropriate online contact with adults/ strangers
- Potential or actual incidents of grooming
- Online bullying.
- The additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.

Through this training, the DSL/DDSL will provide regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

The DSL/DDSL will ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy. They will liaise with other agencies and/or external services if necessary

Network Manager/ Technical Staff

It is the responsibility of the school to ensure that the outside contractor carries out all of the online safety measures that the school's obligations and responsibilities require. The provider should follow and implement the Online Safety Policy and procedures.

At Gunthorpe, our network and services are provided by RM Education. They are responsible for ensuring that:

- They are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- The school technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets (as a minimum) the required online safety technical requirements as identified by the local authority/Aspire or other relevant body

- There is clear, safe, and managed control of user access to networks and devices , including setting up passwords.

- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- Filtering is applied and updated on a regular basis and according to the age of the user.

- Monitoring software/systems are implemented and regularly updated as agreed.

All Staff

Staff should ensure that all information in this policy is read and understood. If anything is not understood it should be brought to the attention of the Headteacher.

Staff should have an up-to-date knowledge of current online safety issues, recognising that this is central to the safeguarding of all children. Any e-safety incidents (including suspected misuse) should be reported to the SLT/DSL immediately, in line with safeguarding procedures. They should model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.

They will agree and adhere 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). They should follow the correct procedures by alerting RM if they need to bypass the filtering and monitoring systems for educational purposes.

Parents/carers

Parents/carers are expected to:

Notify a member of staff or the headteacher 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). This will also be shared with children in school, at the start of each academic year.

Engage with communications sent home, and in information via our website, about children's safe use of the internet and technology.

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

Parent resource sheet – Childnet

Cyber-bullying

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

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 also 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.

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

Artificial intelligence (AI)

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

Gunthorpe recognises that AI has many benefits to offer, however, it also has 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.

Children are taught critical evaluation skills for AI-generated content (e.g. fake news, misinformation) through the curriculum.

Gunthorpe will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to abide by a code of conduct regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use codes of conduct in appendices 1 to 3.

Pupils and mobile devices in school

Pupils are not permitted to have mobile phones at school unless this has been agreed with the Headteacher.

Smart watches should not be brought to school: they may be valuable and could be lost or stolen. Any Smart watches worn by children must not have any internet connection whilst in school.

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 6 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol), where applicable.
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

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 RM.

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 ICT and internet acceptable use. 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 Disciplinary Procedure (including Allegations Against Staff and 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.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4. They also run a monthly filtering report (testfiltering.com) and share any issues with RM.

Appendix 1: EYFS and KS1 acceptable use code of conduct (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: CODE OF CONDUCT FOR PUPILS AND PARENTS/CARERS

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select 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
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Parent/carer code of conduct: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Appendix 2: KS2 acceptable use code of conduct (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: CODE OF CONDUCT FOR PUPILS AND PARENTS/CARERS
I will read and follow the rules in the acceptable use code of conduct. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a member of staff is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity or as part of GOSH (Gunthorpe Out of School Hours) • Use any inappropriate language when communicating online • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to anything using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**
Parent/carer's code of conduct: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Appendix 3: acceptable use code of conduct (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: CODE OF CONDUCT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
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 that 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

Appendix 4: online safety incident report log

GUNTHORPE C OF E PRIMARY 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**

Appendix 5: Mobile phone and smart watch use

The aim of this document is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice through establishing clear and robust acceptable mobile user guidelines. This is achieved through balancing protection against potential misuse with the recognition that mobile phones and smart watches are effective communication tools. This applies to all individuals who have access to personal mobile phones and smart watches on site. This includes staff, volunteers, governors, children, young people, parents, carers, visitors and contractors.

Personal Mobiles and Smart Watches

Staff/Volunteers/ Peripatetic teachers/Visitors/Governors are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office. All volunteers, visitors, governors and contractors are expected to follow our mobile phone and smart watch policy as it relates to staff whilst on the premises. All visitors will be informed of our expectations around the use of mobile phones/smart watches.

- Staff should have their phones on silent or switched off and out of sight (e.g. in a bag, drawer or cupboard) during class time. Smart watches can be worn during school day by staff but the camera, messaging and call services must be disabled.
- Mobile phones should not be used in a space where children are present (e.g. classroom, playground).
- Use of phones (including receiving/sending texts and emails on smart watches and mobile phones) should be limited to noncontact time when no children are present e.g. in office areas, staff room, empty classrooms.
- Should there be exceptional circumstances (e.g. acutely sick relative), then staff should make the Head teacher aware of this and arrangements will be made with the school office so that the emergency call can be received.
- Staff are not at any time permitted to use recording equipment on their mobile phones/smart watches, for example: to take recordings of children, or sharing images. Legitimate recordings and photographs should be captured using school equipment such as cameras and iPads.
- It is recognised that a smart watch may be visible on an adult's wrist, but they must be in silent mode and not used during the working day other than to read the time
- Staff should report any usage of mobile devices that causes them concern to the Headteacher.
- While we would prefer parents and carers not to use their mobile phones whilst at school, we recognise that this would be impossible to regulate and that many parents see their phones as essential means of communication at all times. We therefore will ask that parents' and carers' usage of mobile phones, whilst on the school site, is courteous and appropriate to the school environment. We also allow parents and carers to photograph or video school events such as shows or sports day using their mobile phones/tablets if there are no parental objections or safeguarding issues, – but insist that parents do not publish images (e.g. on social networking sites) that include any children other than their own.

Mobile Phones for work related purposes

- We recognise that mobile phones provide a useful means of communication during offsite activities. However, staff should ensure that:
- Mobile use on these occasions is appropriate and professional.
- Mobile phones should not be used to make contact with parents during school trips – all relevant communications should be made via the school office.
- Where parents are accompanying trips they are informed not to make contact with other parents (via calls, text, email or social networking) during the trip or use their phone/smart watch to take photographs of children.

- Staff taking photos of children during a trip must upload them to the school's system immediately and delete them from their personal mobile devices without delay.

Personal Mobiles and Smart Watches for children

- We recognise that mobile phones/smart watches are part of everyday life for many children and that they can play an important role in helping pupils to feel safe and secure. However, we also recognise that they can prove a distraction in school and could provide a means of bullying or intimidating others. Therefore pupils are not permitted to have mobile phones at school unless they have had prior consent from the Headteacher.
- Smart watches should not be brought to school, they may be valuable and could be lost or stolen. Any Smart watches worn by children must not have any internet connection whilst in school.

Tracking, Apple Airtags or equivalent (School Trips)

Apple air tags or equivalent should not be attached to pupils/belongings going on school trips or residential trips. This is safeguarding decision.

Tracking devices undoubtedly offer a layer of security, especially in crowded spaces such as festivals or Theme parks, however, it's crucial not to misuse them for overbearing surveillance over children. Consideration should be given to create safe environments for children, as they explore their space. School trips and residentials are risk assessed and always supervised by experienced staff. Staff value your trust and support with offering your children these out of school experiences.