GREAT CHESTERFORD C. OF E. PRIMARY ACADEMY

Two are better off than one, because together they can work more effectively.

Ecclesiastes 4:9

Online Safety Policy

Contents

'Together we are great'

At Great Chesterford C. of E. Primary Academy, we aim to provide the best possible education for each child within the context of a caring Christian community. Our school values underpin all aspects of school life, including behaviour and relationships within our school. Our school values are: God's Guidance, Respect One Another, Excellent Behaviour, Aiming High and Tremendous Teamwork. Our golden rule is to 'Treat others as you would like to be treated.'

.

Computing, of which e-safety and safe use of the Internet is an integral element, is taught as part of a broad and balanced curriculum, which will enable each child to develop confidently and learn and achieve to the best of his/her ability in a safe environment. The Internet is part of everyday life for education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience. Pupils will be taught how to use the Internet safely and show a mature and responsible approach to its use. Pupils will use age-appropriate tools to research internet content and be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

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

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, anti-Semitism, 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 scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The Governing 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).

The governor who oversees online safety is Joanna Hancock as Safeguarding Governor.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead

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

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- 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 policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or Governing Body as required.

3.4 The ICT manager

The ICT manager is responsible for:

- Liaising with Essex County Council to ensure that the school has appropriate security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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 monthly basis
- Blocking access to potentially dangerous sites, reporting evidence where access to potentially dangerous sites has occurred and, where possible, preventing the downloading of potentially dangerous files
- 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 dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

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 (appendices 1 and 2)
- Working with the DSL 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 policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents 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)

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 resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody
- Our school website www.greatchesterfordprimary.co.uk under the 'Parents' tab.

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 3).

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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- 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. 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 or access external advisors (e.g. Crucial Crew, the 2 Johns). Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND. The teaching of the computing curriculum will be monitored by the Computing Co-ordinator in liaison with teaching staff.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. Annual parent information evenings will be provided to support parents in keeping their children safe. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings on an individual basis as required.

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

Concerns or queries about this policy can be raised with any member of staff, the headteacher or a member of the Governing Body.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school anti-bullying policy.)

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. This includes personal, social, health and economic (PSHE) education and computing, and other subjects where appropriate.

All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

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

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*

* Staff may also confiscate devices for evidence to hand to the police if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

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

7. Acceptable use of the Internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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. RM Safetynet monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Remote Learning

The purpose of remote learning is to ensure that children can still access activities to support their development in line with the expectations of the Early Years Foundation Stage or National Curriculum and our whole school curriculum map. Class emails or Teams may be used to allow parents to communicate directly with the class teachers about remote learning and for class teachers to offer guidance and feedback to the pupil who completed the work.

Please see the Remote Learning policy for further details of our approach.

9. Pupils using mobile devices in school

Pupils may not bring Internet-enabled mobile devices into school unless by arrangement with the class teacher. Examples include:

- Mobile phones
- iPods
- Tablets
- Kindle Fires
- Smart watches

Any such item brought into school without prior arrangement will be confiscated and then returned to their parent / guardian. If a child needs to bring in a mobile device, it will be kept in an agreed safe place during the school day.

10. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected with a strong password which is not shared with anyone.
- All sensitive documents must also be password protected if stored on the device's hard drive.
- Making sure the device locks if left inactive for a period of time

Staff must take all reasonable steps to ensure the security of their work device when using it outside of school. Any USB devices containing data relating to the school must be encrypted.

The IT support team will be responsible for ensuring anti-virus software is up to date and operating systems are also updated. Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3. If staff have any concerns over the security of their device, they must seek advice from Interm IT, the school's IT support.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the Internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary

procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

This policy will be shared with all new members of staff as part of their safeguarding training. All staff will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required for example through emails, e-bulletins and staff meetings.

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, 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 the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection policy.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This online safety policy is linked to our:

- Child protection policy
- Behaviour policy
- Staff conduct policy
- Data protection policy and privacy notices

- Complaints procedure
- Policy for remote learning
- Computing policy

15. Evaluation, Review and Revision

This policy was written in October 2021. This policy will be reviewed annually by the Headteacher in consultation ith the staff and governors.

Signed: Headteacher	October 2021
Signed: On behave of the Governing Body	October 2021
Next Review Date:	September 2022

Appendix 1: Acceptable use agreement (pupils and parents/carers)

GREAT CHESTERFORD C. OF E. PRIMARY ACADEMY Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will: 1. I will use the school computers / laptops, iPads, iPods, Internet, and all other technological equipment sensibly and for educational purposes. 2. I will ask permission from an adult before using the Internet or school devices. 3. I will not enter chat rooms or leave messages on bulletin boards whilst using school devices. 4. If I see anything I am unhappy with or I receive messages I do not like, I will tell an adult immediately. 5. I will look after the school IT equipment and tell an adult straight away if something is broken or not working properly. 6. I will never share my personal details, home address or telephone numbers with anyone without the permission of my teacher, parent or carer. 7. I will only use my online learning accounts and will keep my passwords safe. 8. Check with my teacher before I print anything. 9. I will be polite and use appropriate language when communicating online. 10. I will always log off and shut down the laptop 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.**	
Signed (pupil):	**Date:**
Parent/carer agreement: As the parent or legal guardian of the child signing above, I grant permission for my child to use electronic mail and the internet. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the internet may be objectionable and I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information and media.	
Signed (parent/carer):	**Date:**

Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)

GREAT CHESTERFORD C. OF E. PRIMARY ACADEMY

Acceptable use of the school's ICT systems and internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, 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
- 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
- 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

During school hours, I will only use the school's ICT systems and access the internet in school for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

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.

I will not use my own personal devices, including mobile phones, to record or photograph children without consent from the headteacher.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Please note: The school strongly advices staff, governors, volunteers and visitors not to become "friends" with pupils or other under-aged children on social networking sites.

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**