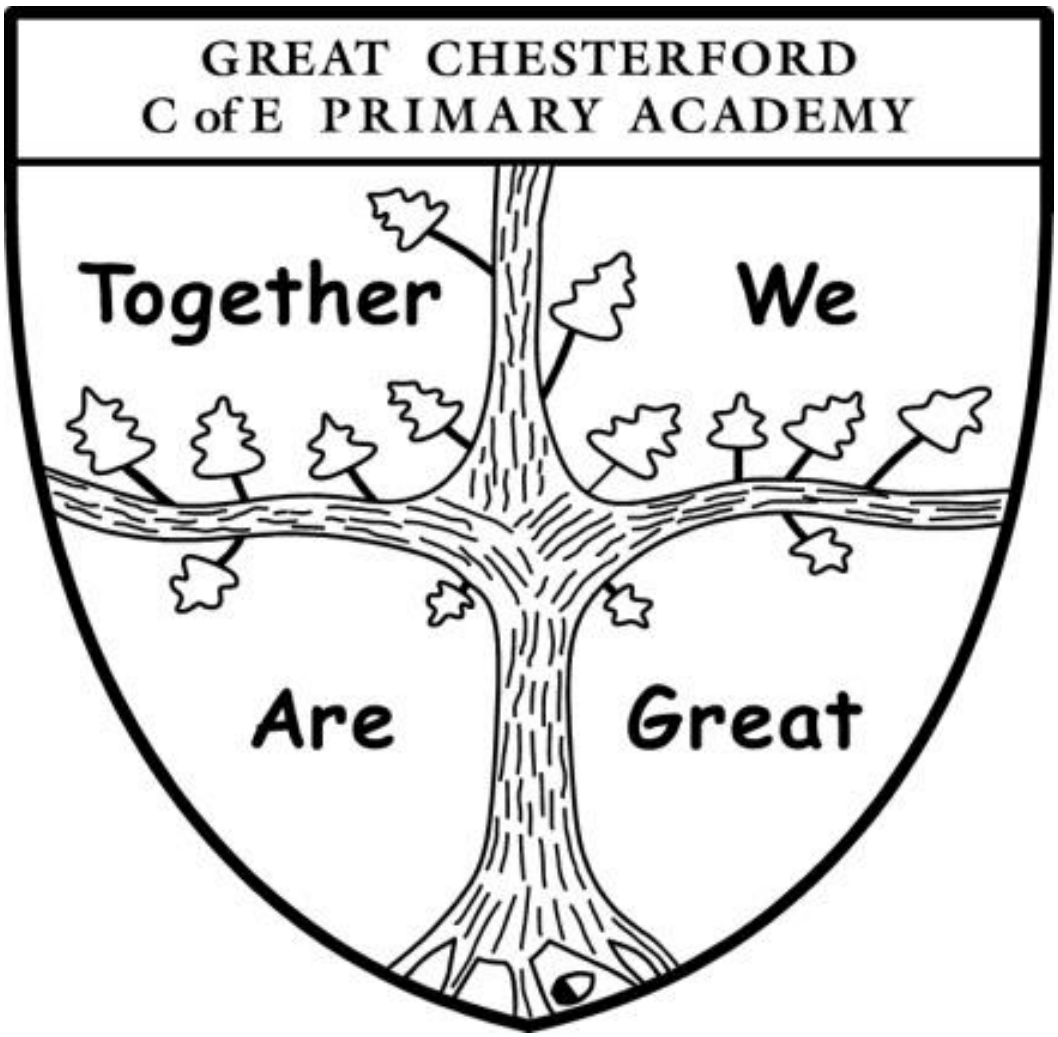
GREAT CHESTERFORD C. OF E. PRIMARY ACADEMY



Online Safety Policy

Approved by the Full Governing Body March 2018

'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.

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 purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet
- Describe how these fit into the wider context of our behaviour, safeguarding and PSHE policies
- Demonstrate the methods used to protect children from sites containing inappropriate material
- Offer guidance about the use of social networking sites.

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

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

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

Using the Internet to enhance education

The benefits include:

- Access to a wide variety of educational resources in order to enrich the curriculum;
- Rapid and cost-effective world-wide communication;
- Staff professional development through access to new curriculum materials, expert knowledge and practice;

- Exchange of curriculum and administrative data with the Local Authority and DCSF;
- Developing their digital Literacy skills for secondary school and beyond.

Roles and Responsibilities

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).

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)

The headteacher

The headteacher, as designated safeguarding lead (DSL), is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The DSL takes lead responsibility for online safety in school, in particular:

- Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing reports on online safety in school to the governing body as required

The ICT manager

The ICT manager is responsible for:

- Liaising with Essex County Council to ensure that appropriate filtering and monitoring systems are in place, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting security checks and monitoring the school's ICT systems on a monthly basis
- Report any evidence where access to potentially dangerous sites has occurred and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any incidents of cyber-bullying or inappropriate use of online content are reported to the DSL.

All staff and volunteers

All staff (including contractors and agency staff) and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the Internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL 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

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 (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf
- Our school website www.greatchesterfordprimary.co.uk under the 'Parents' tab.

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or Internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

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

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 teaching of the computing curriculum will be monitored by the Computing Co-ordinator in liaison with teaching staff.

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.

Cyber-bullying
The school's anti-bullying policy outlines our approach to dealing with any incidents of Cyber-bullying. Our curriculum makes provision to educate the pupils in an awareness of cyber-bullying and its management. All teaching staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
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 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.

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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

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 and 2). 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.
Essec County Council 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 and 2.

Communication and video conferencing
All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer. Pupils will ask permission from a teacher before making or answering a

videoconference call. Videoconferencing will be supervised appropriately for the pupils' age and ability. Parents and carers consent should be obtained prior to children taking part in videoconferences.

Pupils using mobile devices in school

Pupils may not bring internet-enabled mobile devices into school. Examples include:

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

Any such item brought into school by a child will be confiscated and then returned to their parent/guardian.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT system or Internet, we will follow the procedures set out in the behaviour policy.

Where a staff member misuses the school's ICT system 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.

Training

This policy will be shared with all new members of staff as part of their safeguarding training. 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, e-bulletins and staff meetings).

The DSL and the deputy DSL 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 have access to training on safe Internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy

- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Evaluation, Review and Revision

This policy was written in February 2018. This policy will be reviewed annually by the headteacher in consultation with the staff and governors. At every review, the policy will be shared with the Governing Body.

Signed: Headteacher	Date:
Signed: On behalf of the Governing Body	Date:
Next Review Date:	

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:	

In order to keep ourselves and others safe, I agree to the following:

1. I will use the school computers/laptops, iPads, iPods, Internet, and all our technological equipment sensibly.
2. I will ask permission from an adult before using the Internet.
3. I will not enter chat rooms or leave messages on bulletin boards at school.
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 never share my personal details, home address or telephone numbers with anyone without the permission of my teacher, parent or carer.
6. I will only e-mail people or open e-mails from people I know or my teacher/parent has approved.
7. I will always be polite and use appropriate language when sending e-mails.
8. I will not look at or delete other people's files without their permission.
9. I will only use my online learning accounts and will keep my passwords safe.
10. I know that the school may check my computer files, monitor the Internet sites I visit and filter the contents of my e-mails.
11. I understand that if I deliberately break these rules, I could be stopped from using the school network and accessing the Internet.

Signed (pupil):	**Date:**

Parent/carer agreement: As the parent or legal guardian of the child signing above, I grant permission for my son/daughter 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/guardian):	**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/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. • Use them in any way which could harm the school's reputation. • Use them in any way which could breach confidentiality. • Use any improper language when communicating online, including in emails or other messaging services. • Install any unauthorized software. • Share my password with others or log into the school's network using someone else's details.	
During school hours, I will only use the school's ICT systems and access the Internet in school for educational purposes or the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password protected when taking 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 that they have found any material which might upset, destress or harm them or others, and I 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 (pupil):	**Date:**
Please note: The school strongly advises staff, governors, volunteers or visitors not to become "friends" with pupils or other under-aged children on social networking sites.	

Appendix 3 – online safety incident report log

Great Chesterford C. of E. Primary Academy Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**