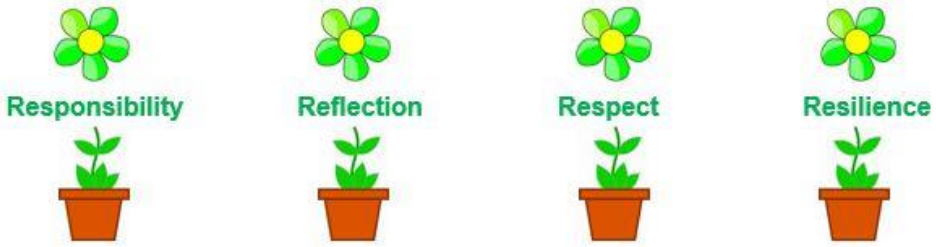
Online Safety Policy

Inspire, Achieve, Shine

Curriculum Vision Statement:
Our curriculum vision is to develop a lifelong love of reading and learning. To enable our children to be healthy, happy and prepared for the future.
Our aim is to broaden the children's horizons and opportunities in the world we live in.

Our curriculum is underpinned by our core values:



Chair of Governors:	Mary Braham	**Signed:**
Chair of Committee:		
Committee Responsible:	SLT	
Staff Responsible:	Chloe Rodwell	
Date Reviewed:	January 2024	
Next Review:	September 2024	
Upload to Website:		**Date Uploaded:**

Version	Review Date	Changes Made by	Sections affected	Changes

Contents

1. Aims

Great Doddington Primary 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
- Ensure that all pupils are protected against risks online, including content, contact, conduct and commerce (the 4 Cs)

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

KCSIE (2021) states that technology is a component in many safeguarding issues and abuse can happen online, offline or both. Children can also abuse their peers online. This can include:

- Abusive, harassing or misogynistic messages
- Non-consensual sharing of indecent images (particularly in chat groups)
- Sharing of abusive images and pornography to those who don't want to receive such content.

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.

The policy also takes into account the National Curriculum computing programmes of study. Pupils at Great Doddington Primary School will be taught about cybercrime as children whom are particularly skilled in computing and technology may be drawn into cybercrime either deliberately or inadvertently. KCSIE defines cybercrime as criminal activity committed using computers and/or the internet, this include hacking, 'denial of service' and creating or using malware such as viruses.

Childline explains the 4 Cs of online safety as:

- Content: anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact: the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.
- Conduct: the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.
- Commerce: the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.

3. Roles and responsibilities

3.1 The Governing Body

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

The governor who oversees online safety is Richard Ward.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms of the school's Acceptable Use Policy

3.2 The Head Teacher

The Head Teacher 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 and safeguarding policy.

The DSL and the Computing Subject Leader take lead responsibility for online safety in school, in particular:

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head Teacher, IT Technician and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on MyConcern 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 cyber-bullying 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 Head Teacher and/or governing body
- Annually review the policy, alongside the computing subject leader

3.4 The Computing Subject Leader

The Computing Subject Leader and DSL take lead responsibility for online safety in school, in particular:

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head Teacher, IT Technician and other staff, as necessary, to address any online safety issues or incidents
- Annually review the policy, alongside the DSL
- Alongside SLT, annually review current risks that pupils may face online using an online safety audit and risk assessment (LGfL)

3.5 The IT Technician and IT Support Company

The IT Technician is responsible for:

- Putting in place appropriate filtering and monitoring systems, 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 a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Supporting the DSL and computing subject leader with online safety incidents
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school cyber-bullying policy

3.6 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 of the schools Acceptable Use of Technology policy
- Working with the DSL to ensure that any online safety incidents are logged on MyConcern
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school cyber-bullying policy

3.7 Parents

Parents are expected to:

- Notify a member of staff or the Head Teacher of any concerns or queries regarding this policy
- Ensure their child (KS2) 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 by viewing the online safety section of the school's website

3.8 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 school's Acceptable Use of Technology policy

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

The Purple Mash scheme of work includes comprehensive online safety units for all year groups.

The safe use of social media and the internet will also be covered when relevant.

The school may 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.

By the end of Year 6 at Great Doddington 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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home (Great Doddington Newsletters), and in information via our website. This policy will also be shared with parents.

Great Doddington Primary School may host an online safety parent workshop once per academic year.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL, Head Teacher or computing subject leader.

6. Training

All staff members will receive relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and Computing Subject Leader will attend online safety training regularly.

Volunteers will receive appropriate training and updates, if applicable.

7. Monitoring arrangements

The DSL monitor concerns raised relating to online safety and shares with the computing subject leader. All staff should record online safety incidents on MyConcern.

Great Doddington Primary School uses MyConcern to record and manage safeguarding concerns. MyConcern is a secure safeguarding software.

8. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding policy
- Behaviour policy
- Staff Handbook

- Acceptable Use Policy
- Filtering and Monitoring Policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS	
Class:	

When I use the school's ICT systems (like ChromeBooks) 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 click on 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
• I will 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.	

Signed (Class Teacher)	**Date:**
Pupil names	

To be discussed and agreed as a class.

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **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 teacher is present, or with a teacher's permission • Keep my username 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 which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network 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.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: 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.	

All KS2 pupils to sign individually. A copy to be sent to parents.