Cledford Primary School and Gainsborough Primary & Nursery School

The Sercombe Federation

George VI Avenue, Middlewich, Cheshire, CW10 0DD
Telephone: 01606 288240
E mail: admin@cledford.cheshire.sch.uk
Website: www.cledford.cheshire.sch.uk

Local Authority Code: 895
Establishment Number: 3821

School Principal: Mr C Adlington

Belgrave Road, Crewe, Cheshire, CW2 7NH
Telephone: 01270 696810
E mail: admin@gainsborough.cheshire.sch.uk
Website: www.gainsboroughschool.co.uk

Local Authority Code: 895
Establishment Number: 3810

Federation Headteacher: Mrs A J Booth

School Principal: Mrs J Nurse

Online Safety Policy

Reviewed: March 2024

Signed:

Mrs J Sercombe (Chair of Governing Board) …….

Mrs AJ Booth (Federation Headteacher) …….

Mrs J Nurse (School Principal GPNS) …….

Mr C Adlington (School Principal CPS) …….

Next Review Date: March 2025

1. Online Safety: The Rationale

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies enhance communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children need to be used effectively and safely.

Online safety includes the use of new technologies, internet and electronic communications such as Learning Platforms, collaborative learning tools and personal publishing. It highlights the need to educate pupils about the benefits and the risks of using technology and provides safeguards and awareness for users to help them control their online experiences. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE) and other statutory documents.

This policy accounts for all existing and developing technologies used within Gainsborough Primary School and Cledford Primary School. It forms part of the School Development Plan and will operate alongside other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Security.

Online safety depends on effective practice at a number of levels:

- Responsible computing use by all staff and students; taught primarily through the Purple Mash software which includes year group overviews, planning, resources and lesson outlines. This may also be supplemented by other resources.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from an approved ISP using suitable filtering and monitoring.
- Parent support, cooperation and reinforcement of following online safety expectations.

2 Writing and Reviewing the Online Safety Policy

- Our schools will appoint an Online Safety Co-ordinator/subject lead who will liaise closely with the Designated Safeguarding Lead as and when necessary.
- The Online Safety Policy has been written by the school, building on government guidance. It has been agreed by Senior Management and approved by the school governing board.
- The Online Safety policy and its implementation will be reviewed annually or earlier if deemed necessary.

3 Teaching and Learning

Why Internet Use is Important

- The Internet is an essential element for education, business, and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils. The internet is essential to provide children with the skills needed to access a rapidly progressing society.

How is online safety embedded in our curriculum?

- Purple Mash will be used as the primary source for lessons, planning and progression.
- Age appropriate lessons are taught within all year groups. Early Years and Key Stage 1 learn how to keep their passwords private and about their digital footprint. Lower Key Stage 2 learn about PEGI ratings for games and Apps, understanding not everything they see on the internet is true, phishing and screen time. Upper Key Stage 2 are taught to critically evaluate the materials they read and shown how to validate information before accepting its accuracy.
- All children are taught about appropriate online behaviour, in year 6 children are taught about how their behaviour online can impact others, and that their link to their digital footprint can have a long-lasting impact.
- Online Safety workshops are delivered to all classes using CEOP resources.

4 Managing Internet Access

Information System Security

- The school IT systems and security will be reviewed regularly
- Suitable virus protection is installed on every networked computer and is updated automatically.

E-Mail

- Pupils are required to inform their teacher immediately if they become aware/receive offensive e-mails/material.
- Pupils must not reveal personal details of themselves or others in e-mail or MS Teams communication.
- Pupils are taught about the appropriate use of e-mail facilities and all external communication will be authorised before sending.
- Any e-mail accounts are strictly monitored by designated super users.

5 Published Content and School Website

- The contact details provided on the website are the school address, e-mail and phone/fax numbers. No staff or pupils' personal information is published.
- The designated super users of the Learning Platform will take overall editorial responsibility and ensure content is accurate and appropriate.

6 Publishing Pupils' Images and Work

- Parental consent forms must be completed by parents prior to any images of children being published.
- Pupil's full names will not be used anywhere, particularly in association with photographs.
- When photographs are used, they will be selected carefully and will not enable individual pupils to be clearly identified unless permission has been provided.
- Any images of pupils will be taken on school electronic devices such cameras or iPads. Staff will not use their own personal recording equipment such as mobile phones for taking or storing images.

7 Social Networking and Personal Publishing

Social Networking sites are designed to engage children and it is important that the children at Gainsborough Primary School and Cledford Primary School are made aware of the potential risks of using these sites.

- The school will block access to all public social networking sites through the school filtering system.
- Pupils will be taught about suitable use of any social networking system (including blogs) through our website and Purple Mash software.
- Pupils are taught to never share personal details or information of any kind which may identify them, their location or any logon information.
- If used, newsgroups will be blocked unless a specific use is approved, for example a forum set up by a teacher on the Learning Platform.

8 Managing Filtering

- The school will work alongside the LA, DCFS and the ISP to ensure systems to protect pupils are reviewed and improved.
- Any unsuitable sites that are discovered by staff or pupils must be reported to the school's Online safety co-ordinator and Designated Safeguarding Lead.
- Effective filtering and monitoring through software installed on every computer in the school. Where an inappropriate search takes place on any device or account, an automatic report will be sent to the Principal, so the incident can be followed up quickly and efficiently.

9 Managing Emerging Technologies

As new technology emerges, it is important that we understand the technology rather than ban it without any forethought, by considering its use carefully we are educating the pupils on safe and effective use.

- The educational benefit of emerging technologies will be considered and a risk assessment will be carried out before school use is permitted.
- New technologies and websites may be used at the discretion of the teacher.

10 Protecting personal data.

- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 1998.

11 Policy Decisions

Authorising Internet Access

- All staff must read and sign 'Online Safety Agreement' before using any school computing resource.
- All parents and pupils will be asked to read, agree, sign and return a consent form with respect to acceptable use of the technologies available.
- All consent forms will be kept in file and the record will be updated as appropriate.
- Pupils' internet access within school will be supervised and monitored at all primary stages.
- When logging onto the system, children will need to accept a safe-use policy, before being able to access the computer.

12 Remote learning

- In any exceptional circumstance, a child may need to undertake remote learning. They would be expected to take part in online learning through Microsoft Teams.
- When children access remote learning, at least two members of staff (when possible) are to be present during live lessons.
- Children will access lessons through their log on provided by the school office.
- Staff, children and supervising parents must dress appropriately when conducting online lessons as they would in school.
- Parents will receive a 'how to' guide with guidelines and expectations for their children to follow when taking part in online lessons.
- Pupils are expected to behave as they would in classrooms.
- Staff should not leave children unmonitored on Microsoft Teams – breaks which have been allotted should be used where video calls have ended.
- Children are expected to complete and 'hand in' work either virtually or record it in their home learning books as they would in school with high expectations on presentation.
- Be situated in a suitable working environment which is as quiet as possible, well-lit and has enough space to complete written and computer-based activities.
- Use appropriate language – this includes others in their household.
- Any recording or screenshotting is prohibited by children. Not record, store, or distribute video material without permission.
- Lessons may be recorded by staff if there is a safeguarding concern.
- The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.
- The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

13 Online Behaviour

- Our expectations of all children is that their behaviour online should replicate their behaviour in school, and follow our 3 rules: be ready, be respectful and be safe.
- We have clear and robust safeguarding procedures in place for responding to any online misbehaviour or online abuse.

In School

- Pupils not using devices or software as intended will be disciplined in line with the Behaviour Policy.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the Local authority can accept liability for the material accessed, or any consequences of internet access.
- Any complaint about staff misuse must be referred to the Headteacher.
- There is support and training for all staff on dealing with bullying or cyberbullying.
- Our response to online misbehaviour will take the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account.
- A review of the plan developed to address online abuse will take place at regular intervals, in order to ensure that any problems have been resolved in the long term.

Out of School

- We support and encourage children to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.
- We support and encourage parents and carers to do what they can to keep their children safe online, this includes informal conversations and workshops for parents delivered in school.
- Low risk reports of online safety concerns will be explored in school. Further online safety teaching for the child will take place in school. Support and advice will be given to parents to ensure children are safe online at home.
- Higher risk reports of online safety concerns will be investigated by a senior member of staff. Parents will be invited into school to discuss how we can ensure their child is safe online and no further similar incidents occur.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

15. Community use of the Internet

- The school will liaise with local organisations to establish a common approach to Online Safety.
- PCSO officers to liaise with the school and provide an Online Safety talk to children in KS2.

16. Communications Policy

- Online safety rules will be posted in all networked rooms and discussed with the pupils at the start of each term.
- Pupils will be informed that network, website and Internet use will be monitored.
- All staff will be aware of and able to access the online safety policy and its importance explained.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Parents' attention will be drawn to the school online safety policy in newsletters and school website.

Online Safety - Keeping Children Safe in Education (KCSIE)

As per government guidance, the teaching and learning of the 4 C's (content, contact, conduct and commerce) is taught through our computing curriculum and PHSCE curriculum. These topics are taught discreetly and revisited throughout KS1 and KS2 at a level appropriate to the children's understanding.

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content. In all cases, if staff are unsure, they should always speak to the designated safeguarding lead (or deputy).

Staff must be aware that abuse can take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults or by another child or children. Sexual abuse can take place online, and technology can be used to facilitate offline abuse.

An outline of the 4C's:

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, 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.

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users; for example: 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.

Commerce – risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Online safety agreement

Parents/carers: please read and discuss this agreement with your child and then sign it, ask your child to sign it, and return it to the school office.

Young person's agreement

- ✓ I will be responsible for my behaviour when using the internet, including social media platforms, games and apps.
- ✓ I will always use kind language.
- ✓ I will not share my passwords with anyone.
- ✓ I will not give out any personal information online, such as my name, phone number, address or a photograph of myself wearing school uniform.
- ✓ I will only talk to my friends that I have met in real life.
- ✓ I will not deliberately browse, download or upload material that could be considered offensive or illegal.
- ✓ I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- ✓ I understand that my internet use at Gainsborough/Cledford will be monitored by my teachers.
- ✓ If I am worried or upset about anything I see on the internet or any material or messages that I receive, I know I should tell a trusted adult.
- ✓ I understand that these rules are designed to keep me safe and that if I choose not to follow them, Gainsborough may contact my parents/carers.
- ✓

Signatures:

We have discussed this online safety agreement and _____ (child's name) agrees to follow the rules set out above.

Parent/carer signature..... Date .....

Young person's signature..... Date .....