



Cledford Primary School

George VI Avenue, Middlewich, Cheshire, CW10 0DD
Telephone: 01606 663667
E mail: admin@cledford.cheshire.sch.uk
Website: www.cledford.cheshire.sch.uk

Gainsborough Primary & Nursery School

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: 3821

Local Authority Code: 895
Establishment Number: 3810

School Principal: Mr C Adlington Federation Headteacher: Mrs A J Booth School Principal: Mrs J Nurse

Federation Online Safety Policy

Reviewed: March 2023

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' 2022 (KCSIE) and other statutory documents.

This policy accounts for all existing and developing technologies used within Gainsborough Primary & Nursery 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.

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.

Internet Use Will Enhance Learning

- Purple Mash will be used as the primary source for lessons, planning and progression evaluation.
- Pupils should be taught to critically evaluate the materials they read and shown how to validate information before accepting its accuracy.

4 Managing Internet Access

Information System Security

- The school IT systems and security will be reviewed regularly every 12 months
- 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 available through the Learning Platform are strictly monitored by designated super users.

5 Published Content and the School Learning Platform

- The contact details provided on the Learning Platform 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 on the Learning Platform 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 as 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 & Nursery 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 internal social networking system and blogging through our Learning Platform 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 Local Authority, Department for Children, Schools and Families and the Internet Service Provider 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.

9 Managing videoconferencing.

Simple point to point video conferencing is available via the Learning Platform as a communication tool. If used.

- Pupils will be taught to use the videoconferencing facility in an appropriate manner.
- Video conferencing usage will be monitored by superusers.

10 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.

11 Protecting personal data.

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

12 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.

13 Remote learning

- All children who have access to the internet are expected to take part in online learning through Microsoft Teams.
- When children are working from home, 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 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.
- Any recording or screenshotting is prohibited by children.
- Lessons may be recorded by staff if there is a safeguarding concern.

Online safety of online lessons

All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are not permitted when children are working from home.
- Wear suitable clothing – this includes others in their household.
- 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.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Endeavour to have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

Pupils not using devices or software as intended will be disciplined in line with the Behaviour Policy.

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.

Assessing Risks

- 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.
- The school will regularly audit computing provision to establish if the online safety policy is adequate and its implementation is effective.

Handling Online Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

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 each year group.

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, Learning Platform 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.

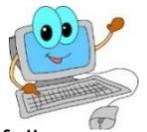


Remote learning guidance for parents

Remote education ensures continuous learning outside the classroom. For parents and carers, remote education is not always straightforward and there can be a number of factors you may need to consider, especially around ensuring your child feels comfortable and familiar learning in this way. The following guidance will help you to maximise the effectiveness of online learning.

Monitor your child's online activity.

It's important to remind your child that despite being at home, the same level of behaviour and conduct exists as if they were at school. Encourage them to remain polite, remember their manners and not to post or send any negative comments.



Establish a daily routine for your child to follow

Working from home and trying to learn in a more casual setting might take a bit of getting used to. Try to follow a daily routine and use the timetable/schedule that has been sent home to help your child to keep on top of their daily learning. The same level of presentation and effort in lessons is expected as it would be in school.



Encourage screen breaks and time away from devices.

Remote learning will require interaction with computers, laptops and tablets. We advise to take lots of breaks from screens and to get some fresh air when possible.

Your child should be in a room free of as many distractions as possible and with enough room to complete tasks such as reading and writing.



Monitor website and applications that your child is using

Teachers may ask children to complete tasks by researching information on safe website which have already been checked for sensitive content. However, parents should make sure that search engines such as 'Google' and other apps have safety restrictions set.



Communication between student and teachers

Communication may only be accessed through Microsoft Teams. Your child has received a unique email address and password which should only be accessed and known to yourselves and not be shared. Communication to teachers will be done only through Microsoft Teams where the children will view their lessons and tasks for the day. No other method of virtual contact will be used.



Monitor your child's mental wellbeing.

Remote education will likely mean that your child won't get the same level of social interaction and might not see their friends for a while. Keep a check on their wellbeing and try to encourage them to get out as much as they can.



Remote Learning Safety Guide for Staff

1. This document sets out guidance when teaching from home and delivering online learning. For staff, there is much to consider to ensure an effective delivery of online lessons. The following guidelines and tips will help to deliver safe, effective, and secure experiences for both teachers and the children.
2. Familiarise yourself with the following policies; Online Safety policy, safeguarding policy, pupil remote learning policy and data protection policy.
3. Consider your surroundings. Ensure that the children can only see yourself and no other adults. Try to have a plain background or use an appropriate background from MS Teams. Ensure that if you are sharing your screen, there is only suitable content visible on your desktop/webpage. Sessions will not be recorded, stored or distributed.
4. In the first session, remind the children of the guidelines which have previously been distributed and discussed in class. Make this clear so that both children and adults know what type of behaviour is expected from them during a lesson.
5. When possible, use school devices to communicate through MS Teams. If using a personal device you must notify a member of SLT. Only use your school MS Teams account to communicate with children to their school assigned email addresses. Only communicate through MS Teams with children in school hours. Do not give out personal emails, numbers or details. When completing pupil phone calls, always hide caller ID.
6. Dress as you would for a working school day. Treat any online lesson as if you were in the classroom. Maintain a professional image and attitude and encourage the children to do the same. Children should not dress in pyjamas.
7. Ensure that children are aware of the class timetable. This will include the number of sessions in a day with the times that the pupils are expected to attend.
8. Ensure that you are using school provided laptop to deliver online lessons. Lessons may only be delivered through MS Teams. If asking children to complete research or any form of internet use, ensure that websites provided have been properly screened before asking children to explore them.
9. Consider the needs of SEN and vulnerable pupils when providing work. Our very vulnerable pupils will need to access learning appropriate to their level. Consider uploading differentiated documents or learning objectives to particular groups of children who would otherwise struggle to access it.
10. As much as possible, try to make lessons fun and engaging. This is an excellent opportunity to use platforms such as Purple Mash to deliver lessons, which are both imaginative and challenging. There are many opportunities to include cross curricular tasks, which link to topic work.
11. If a child divulges information which arouses a safeguarding concern, staff should immediately record the information and pass it on to a member of the safeguarding team while the TA resumes teaching of the online lesson.
12. If an allegation is made about a member of staff, teacher/TA to record what has been alleged. All information of what has been said to be passed on to a member of the safeguarding team **and** the Principal immediately while the TA resumes the lesson.

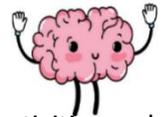


Remote learning Guide for staying safe online

1.) Treat online lessons the same as being in the classroom. Remember many of the rules that you have in the classroom are needed to be followed when you are doing your online lessons. Remember to be respectful and listen to the adult speaking. Try to focus on learning and not get distracted.



2.) Make sure to take breaks away from your computer and other devices. Try to get some fresh air and enjoy other activities when you aren't doing your work.



3.) Make sure you are in a suitable place to work. You will need to have enough room to complete activities such as writing and reading. Make sure that you don't have distractions and that the room you are in is nice and quiet so you can do your best work.

4.) It's important that you only use the websites and apps that your teacher tells you to. This will help to keep your personal information secure.



5.) Be on time for your lessons. Make sure to attend every online lesson on and do not be late! Otherwise, you might miss important information about the lesson.

6.) Dress in suitable clothing to work in. Wear your school uniform if possible. This will make feel more normal to be doing school work and you will look smart!

7.) Do not share passwords or other sensitive information with anyone. You may need to use logon details to get on certain websites such as Purple Mash. Make sure to keep this information private.



8.) Remote education ultimately means working alone and missing out on seeing your friends. If you ever feel frustrated, low or sad, it's important to discuss how you feel with your parents or your teacher.