Christleton Primary School

Be the best you can be

E-Safety Policy

Document name	Author	
E-Safety Policy	Mr Mitchell	
	Version number	1:2
Reviewed by	Controlled copy	X
Full Governing Board	Un-controlled copy	

Date of Policy	Policy Reviewed	Next Review
September 2021		September 2024

Signed Head teacher	
Signed Chair of Governors	

Intent

At Christleton Primary, one of our main aims is that every member of the community feels safe. As a result, this policy must be read in conjunction with all other Safeguarding & Child Protection Policies.
We aim that every member of the school community feels safe and secure using ICT and different technologies at home and at school. We also aim to educate children and parents in how to use ICT safely and appropriately.
Whilst ensuring they understand the advantages and disadvantages associated with online experiences, we want children to develop as respectful, responsible and confident users of technology, aware of measures that can be taken to keep themselves and others safe online.
Our aim is to provide a computing curriculum that is designed to balance acquiring a broad and deep knowledge alongside opportunities to apply skills in various digital contexts.

Implementation

Primarily we will be looking at the internet, but we will also look at other communication tools such as mobile phones. We will highlight both the benefits and risks of using such technologies and provide safeguards as well as awareness so users can control their online experiences.
The Computing Lead and Designated Teacher for Safeguarding (Nia Hughes and Oliver Mitchell) will stay abreast of the most up to date E-Safety and Internet Safety policies and practice.
All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

We will follow the national curriculum for computing which aims to ensure all pupils:

- can understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation (Computer science)
- can analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems (Computer science)
- can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems (Information technology)
- are responsible, competent, confident and creative users of information and communication technology. (Digital literacy)

Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Teaching and Learning

The internet is a vital part of everyday life from education to business. Consequently, it is imperative that school provide children with quality internet access. The internet is a statutory part of the school curriculum.

- The school's internet is filtered appropriately in comparison to the age of our pupils.
- We have the authority to choose which websites are accessible at school.
- The pupils are taught how to use the internet acceptably and are given learning objectives so they know exactly what is expected from them. Pupils are taught how to effectively use search engines to research the internet and are directed towards using the BBC search engines because all their pages have been vetted. In addition to this, pupils are taught how to evaluate the internet content by validating information before accepting its accuracy.
- Any inappropriate websites accessed are passed onto our ICT support (Dan Woolley) who have the ability to block the website. They will also inform the Council's technical service team.
- The school will ensure that the materials used by staff and pupils comply with law.
- All staff will sign the 'Acceptable use agreement and code of conduct.' **(Appendix 2)**

The schools ICT systems capacity and security will be reviewed regularly by following the following steps:-

- Virus protection will be updated regularly by Dan Woolley (ICT Support)
- Security strategies will be discussed with the Cheshire West and Chester Authority, Cosocius and Internet Service Provider.

Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSE
- Health education
- PSHE
- Citizenship
- ICT

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

E-safety Curriculum

All year groups from Reception to Year 6 will have an e safety scheme of work.
http://www.childnet.com/resources/esafety-and-computing/ks1
http://www.childnet.com/resources/esafety-and-computing/ks2

- This scheme of work runs alongside the computing curriculum and the SRE/PSHE curriculums.
- Teachers will teach the E safety scheme of work over a half term or term (it is up to the teacher's discretion, when best to teach the scheme).

Handling online safety concerns

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-Bullying Policy.

Peer-on-peer sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL, who will investigate the matter in line with the Peer-on-peer Abuse Policy and the Child Protection and Safeguarding Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil’s mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents are sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

- Parents' evenings
- Seesaw resources and announcements
- Newsletters
- Online resources

School Website

The aim of the website is to give children, parents, governors and members of the community up to date information about the school. It is also seen as one of the first points of call for prospective parents and as such, needs to maintain the friendly, welcoming feel that Dee Point presents.

Our website will …

- Provide information to our parents through the school website such as newsletters, general letters and dates.
- Provide contact details on the VLP such as the school address, email, telephone number and map. No staff or pupils' personal information will be published.
- Be in line with the current Government expectations for a school website. ***'What maintained schools must publish online'*** (18th September 2015)
- Promote safe use of the internet

- Provide governors access to documentation and a secure area so communication can be regular, private and aid in the school's development.

Website Management

- The Head teacher, Chair of Governors, Computing Lead and ICT support will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website.
- All photos will be re sized to the smallest pixel size before being up loaded onto the internet.
- This permission form will allow teachers and members of staff to publish the children's work.
- No names of children will be used on the public facing pages of the website but some photographs will be used (Similarly to the School Prospectus).
- CPD for relevant staff will be up to date

Social Networking

- The school will manage all access to social media sites.
- Pupils will be instructed not to give out personal details which may identify them or their location. (Part of the E safety schemes of work)
- Pupils and parents will be advised that the use of social network spaces for pupils is inappropriate and that ages restrictions are in place.

Twitter

- The school currently has a Twitter page (@Christletonpri)
- All teachers and teaching assistants have the password to update the twitter account.
- All tweets are public.
- Photos will be public on the account. All parents have the option to opt out of this when their child begins school in Reception or at any time there after by contacting the school office.
- Only reputable Twitter accounts will be followed.
- No parent or pupil accounts will be followed by Christleton Primary School.

Managing Emerging Technologies

- New and emerging technologies will be examined for both educational benefit and risk assessment.
- In emergency situations, staff may be required to use their personal phone to contact emergency services or parents. When contacting parents, staff will use 141 to keep their own mobile phone number private.
- When contacting parents. Staff will use SIMS contacts to ring from school or email, they may also use the Seesaw app.

Protecting Personal Data

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

- Staff may save work, planning and assessment information on a USB or external hard drive to access at home. Any sensitive or personal data, must be securely stored either on an encrypted device, or in a password protected folder. Staff will sign the 'Acceptable use agreement and code of conduct.'
- Staff are also encouraged to use the school OneDrive accounts to save information which are password protected.

Staff Email

- All staff have a personal email account. ______@christletonprimary.cheshire.sch.uk
- All staff use this account for school work use only.
- All staff remain professional at all times through this form of communication.
- If communications about a child are sent through email, initials must be used, so the child is not easily identified.
- All staff will sign the 'Acceptable use agreement and code of conduct.'

Pupil Email

- Pupils currently do not have a personal school email account.
- Pupils may access an email account that is created by their class teacher in order to teach the email area of the curriculum. This account is closely managed by the teacher and the class teacher is responsible for closing the account after use.
- Pupils must immediately tell a teacher if they receive an offensive or inappropriate email.
- Pupils must not reveal personal details of themselves or others in email communication.
- Pupils must not arrange to meet anyone without specific permission.

Internet Access

- KS1 pupils will access the internet through adult led activities. They will be able to access specified internet sites via QR codes, Seesaw or via hyperlinks.
- KS2 pupils will access the internet during Computing lessons as well as during cross curricular lessons.
- All adults will sign the 'Acceptable use agreement and code of conduct.' before using any school ICT resource. A copy of these agreements will be kept by the Computing Lead.
- Any misuse of internet access will lead to immediate internet access withdrawal by the teacher and Computing Lead.
- The school will take all reasonable precautions to ensure that users access only appropriate materials. If this is the case, children will leave the site immediately and staff will add the website to the inappropriate websites list.

E-Safety Complaints

- Complaints of internet misuse will be dealt with by the Senior Leadership Team.
- Any complaint of staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Christleton Primary will follow the Cheshire West and Chester procedures for dealing with significant incidents.

E-Safety Communication

- E-Safety rules will be posted in each class and will be discussed with all pupils through the e safety scheme of work.
- Pupils, Staff and Governors will be aware that internet and VLP usage will be monitored.
- Staff will be informed that the E-Safety Policy will be stored in staff share and staff must read it and adopt it.
- Parents will be directed towards the E-Safety policy in newsletters and via the school website.

Failure to Comply

- Failure to comply with this policy will be investigated by a member of the Senior Leadership Team in line with the Acceptable Use Policy adopted from Cheshire West and Chester (**Appendix 1)**

Seesaw

- All children from Year 1 to Year 6 are allocated a Seesaw account, these accounts can be accessed from home with a home learning log on which is individual to each child.
- Parents have access to their child's account through an individual log on where they are able to view their child's uploads and contact the class teacher.
- Teachers will use the seesaw accounts to contact parents with reminders and relevant updates or reminders.
- The school office will send annual reports through Seesaw as it is a password protected platform.
- All staff are aware of professional conduct expectations on this platform. If staff have any concerns about communication they must inform SLT immediately.

Remote learning

In the event of home learning 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.

Class teachers will use Zoom to deliver live lessons or upload recorded lessons onto Google Drive.

All zoom sessions are password protected, children are required to keep their cameras on throughout the sessions. All sessions will be recorded and kept on the school server.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

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.

Impact

Finding the right balance with technology is key to an effective education and a healthy life-style. We feel the way we implement computing helps children realise the need for the right balance and one they can continue to build on in their next stage of education and beyond. Through constant and open discussion about the use of technology in their day to day lives, we believe the children in our school have a solid understanding of how to stay safe online. We encourage regular discussions between staff and pupils to best embed and understand this. The way pupils showcase, share, celebrate and publish their work will best show the impact of our curriculum. We also look for evidence through reviewing pupil’s knowledge and skills digitally through tools like Seesaw and observing learning regularly.

Appendix 1

(Please refer to Cheshire West and Chester's Acceptable Use Policy)

Appendix 2

Acceptable use policies (AUP's)

- Staff
- KS2
- KS1