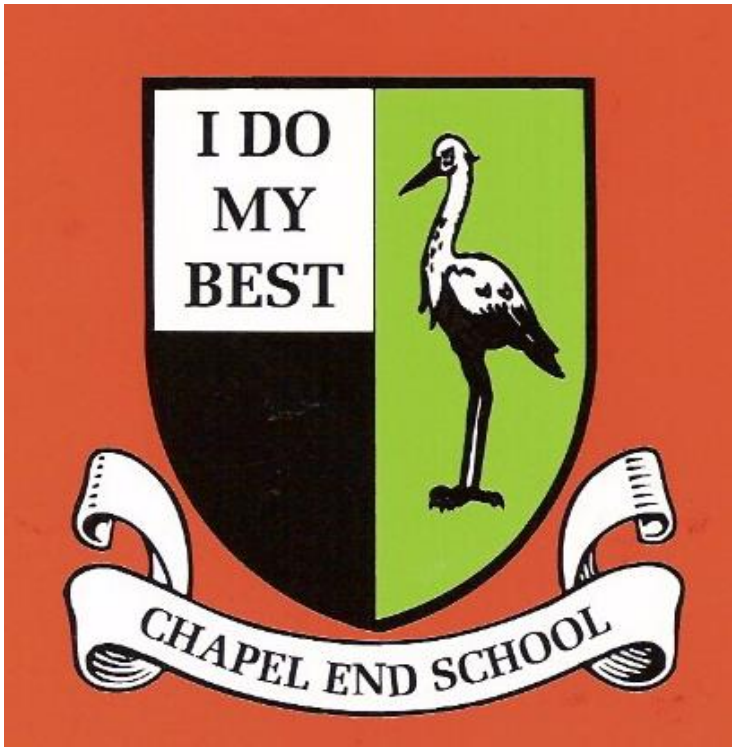

Chapel End Primary School and Nursery E-Safety Policy

'Mission Statement.'

We aim to provide our children with the highest possible standard of education, through quality teaching and learning, in a happy caring environment.

We will do the best WE can to enable our children to do the best THEY can.

This policy was approved by:	Full Governors
Date	Autumn 2020-2021
Review Date	Autumn 2020-2021

Introduction

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. We aim to equip our pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

This policy is supported by:

Teaching online safety in school Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects June 2019

Keeping children safe in education 2020

Working together to safeguard children 2018

Education for a Connected World (UKCIS, 2018)

Context

This policy will include how our children are taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online.

Throughout a range of curriculum subjects and whole school activities, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives. This will complement the computing curriculum (ilearn2), which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies. There are also other curriculum subjects which include content relevant to teaching pupils how to use the internet safely. At Chapel End we are guided by the SCARF citizenship programme of study, which has e-safety embedded. Children learn about media literacy - distinguishing fact from opinion as well as exploring freedom of speech and the role and responsibility of the media in informing and shaping public opinion.

Our curriculum also supports teaching about the concept of democracy, freedom, rights, and responsibilities.

Teaching about online safety

The online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up to date with the latest devices, platforms, apps, trends and related threats. It is therefore important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. At Chapel End Primary School, this teaching is built into existing lessons across the curriculum such as PHSE, covered within specific online safety lessons built into the computing program of study and school wide approaches such as E-safety week. Teaching is always age and developmentally appropriate.

We underpin knowledge and behaviours by teaching the children to:

Evaluate what they see online.

Embedded into our Computing lessons are these key questions:

- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?
- Why does this person want my personal information?
- What's behind this post?
- Is this too good to be true?
- Is this fact or opinion?

Recognise techniques used for persuasion

We aim to enable pupils to recognise the techniques that are often used to persuade or manipulate others.

We support pupils to recognise:

- Online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation),
- Techniques that companies use to persuade people to buy something,
- Ways in which games and social media companies try to keep users online longer (persuasive/sticky design); and
- Criminal activities such as grooming

Online behaviour

At Chapel End, we aim to teach pupils to understand what acceptable and unacceptable online behaviour look like. We teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. Pupils are also taught to recognise unacceptable behaviour in others.

Chapel End Primary helps pupils to recognise acceptable and unacceptable behaviour by:

- Looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do,
- Looking at how online emotions can be intensified resulting in mob mentality,
- Teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online,

• Considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

How to identify online risks

Pupils at Chapel End Primary School are taught to identify possible online risks and make informed decisions about how to act. We focus to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

We do this by:

- Discussing the ways in which someone may put themselves at risk online,
- Discussing risks posed by another person's online behaviour,
- Discussing when risk-taking can be positive and negative,
- Discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e. how past online behaviours could impact on their future, when applying for a place at university or a job for example,
- Discussing how mob mentality describes how people can be influenced by their peers to adopt certain behaviours on a largely emotional, rather than rational, basis,
- Discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with,
- Asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

How and when to seek support

Our aim is to enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

We help pupils by:

- Helping them to identify who trusted adults are,
- Looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation,
- Helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported,
- By applying the principles and procedures detailed in our safeguarding and child protection policies.

Harms and Risks

At Chapel End Primary school we aim to make all of our children aware of the harms and risks associated with the internet. We do this in an age appropriate way using a variety of Curriculum areas as a vehicle for teaching.

These risks include:

- Age restrictions
- Content: How it can be used and shared
- Disinformation, misinformation and hoaxes
- Fake websites and scam emails
- Password phishing
- Personal data
- Persuasive design
- Privacy settings
- Abuse (online)
- Fake profiles
- Grooming
- Live streaming
- Unsafe communication
- Impact on confidence (including body confidence)
- Impact on quality of life, physical and mental health and relationships
- Online vs. offline behaviours
- Reputational damage

Vulnerable pupils

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance. However there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online.

A record of any pupils deemed vulnerable when using online resources is kept securely on the school safeguarding system CPOMS. There is also a link to the Childnet SEN star toolkit on the school website.

Whole school approach

As a school community we aim to:

- Create a culture that incorporates the principles of online safety across all elements of school life.
- Proactively engaging staff, pupils and parents/carers
- Review and maintain the online safety principles
- Embed the online safety principles
- Model the online safety principles consistently

Authorised internet use

The authorised use of internet access is recorded as part of the school's acceptable user policy. All staff and children must agree to, and sign, this document to allow them to access the internet in school. Parents will receive a text message to give them the opportunity to review this permission on an annual basis.

Filtering

The school will work in partnership with parents and St. Helens Council to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable or illegal sites, the URL (address) and content must be reported to the Internet Service Provider (St Helens Council) via the ICT Team and Headteacher/ E-safety officer, Craig Hewitt.

Parents of the children involved will be notified immediately in serious circumstances.

Website logs will be regularly sampled and monitored.

The St Helens ICT Team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Blended Learning

During periods of remote education, all staff, parents and children will adhere to the blended learning policy, safeguarding policy and child protection policy which are displayed on the school website.

To keep staff and pupils as safe as possible the school will:

- Not allow the live streaming of lessons
- Provide parents with specific links to internet sites that have been checked by the teacher.
- Carefully timetable blended learning to allow for screen time breaks.
- Work closely with St Helens ICT team and follow guidance
- Remind parents and children about the e-safety quick link on the school website.

Communication with parents

Parents within the Chapel End Community will be updated with online safety information regularly via the school newsletter. They can access up to date information using the e-safety quick link on the home page of the school website and they will receive opportunities to attend e-safety briefings during parents evenings.

Communication with Staff

This policy will be uploaded to the school CPOM system so it is available to all members of staff. This system will keep a record of staff who have read and understood this policy.

Digital / Video Cameras / Photographs

Pictures, videos and sound are not directly connected to the Internet, but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents and Carers are permitted to take photos/videos of their own child from school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.
- The Headteacher or a nominee will inform parent/s / guardian/s and others present at school events that photographs / videos may be taken on the basis that they are for private retention and not for publication in any manner.

Published Content on the School Website, Facebook and Dojo

The school website is a valuable source on information for parents and potential parents.

- Contact details on the website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- The Headteacher/E-safety officer (Mr Hewitt) and Computing Lead (Mrs Pickett) will take overall editorial responsibility and ensure that content it accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school website.
- Work will only be published with the permission of the pupil.
- Parents should only upload pictures of their own child / children onto social networking sites.
- The Governing Body may ban the use of photographic equipment by any parent who does not follow the school policy.
- Parents/ carers will update consent form which is completed on entry to school indicating how school can publish images of their child. This will be done by a text message being sent to parents at the beginning of each school year asking them to update any changes to the consent form if required.

Mobile technologies

Children

Any child that brings a mobile device to school will hand it in to their class teacher and it will be stored in a secure location for the duration of the school day.

Staff

Staff use of mobile phones during their working day should be:

1. outside of their contracted hours – before or after children are in school or, when they are not on duty during break time or lunch-time
2. discreet and appropriate eg: not in the presence of pupils- for example in the staff room or a private office – if a classroom were to be empty of children at a break time, then the class room would be considered an acceptable place for staff to use their mobile phone
3. Mobile phones should be switched off or left on silent and left in a safe place and out of sight during lesson times. Phones which are left on silent should be protected with a key board lock in case of another person accessing the phone.
4. The school cannot take responsibility for items that are lost or stolen.
5. Staff should never contact pupils or parents from their personal mobile phone or give their mobile phone number to pupils or parents. If a member of staff needs to make telephone contact with a pupil, they should use one of the school telephones.
6. A school mobile will be taken to sporting fixtures away from school or on an educational visit for contacting parents in the event of an emergency. If the school mobile were to be unavailable, staff may use their own mobile phone to contact the school office in case of emergency away from school.

Visitors and Parents

1. Adults either in school or accompanying children on school trips should not use their cameras or mobile phone cameras to take pictures of pupils unless it is at a public event such as sports day or assembly and of their own children.
2. We request that parents do not use mobile phones in the school building or grounds.
3. Adults, visitors or volunteers in school should only use their mobile phone within the confines of the school office or staff room. Personal cameras and mobile phone cameras should not be used to take pictures of children.
4. If parents who accompany children on a school trip are asked by the teacher to take photos as a record of the educational visit, they will be issued with a school camera. Parents accompanying children on school trips should not use their mobile cameras to take pictures of children.

Responding to Incidents of Concern

- The Online Safety coordinator will record all reported incidents and actions taken in the school Online Safety Incident log (CPOMS).
- The Designated Child Protection Coordinator and other appropriate members of staff will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

- The school will manage Online Safety incidents in accordance with the school discipline /behaviour policy where appropriate
- The school will inform parents/guardians of any incidents of concern as and when required
- After any investigations are completed, the school will debrief, identify lessons learned, implement any changes required, and notify the Online Safety group through the Governing Body.
- Where there is cause for concern or fear that illegal activity which concerns an adult has taken place or is taking place then the school will contact the LADO and St Helens LA so that the incident may be communicated to the Police.
- Where there is cause for concern that a child is at risk of significant harm the school will contact the necessary team:

Important contact information:

- Designated Safeguarding Leader: Mr C. Hewitt: 01744678230
- Deputy DSL Mrs K. Trivass: 01744678230
- Chair of Governors: Mr William Bradbury
- St Helens Multiagency Safeguarding Hub: 01744 676 600
- Merseyside Police 999/101/ 0151 709 6010
- St Helens Safeguarding partnership: 01744 671 884