Central Walker
Church of England Primary School

A place to shine …

Let light shine out of darkness and God's light shine in our hearts
2 Corinthians ch4, v6

E-Safety policy

Consultation that has taken place	September 19
Date formally approved by governors	September 19
Date policy became effective	September 19
Review date	September 2021
Person responsible for implementation and monitoring	Jane Caffery
Other relevant policies	Acceptable Use policy Anti-Radicalisation policy

'The name of the Lord is a strong tower; the righteous man runs into it and is safe.'
(Proverbs 18:10)

Introduction
E-safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Anti-Bullying, Curriculum, Acceptable Use, Anti Radicalisation, Data Protection, Safeguarding and Security.

Rationale
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.

The Byron Review, "Safer Children in a Digital World" stressed the role of schools:

"One of the strongest messages I have received during my review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-Safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area." Professor Tanya Byron

At Central Walker Church of England Primary School we believe that it is essential for us to take a leading role in e-Safety. We wish to support our parents in understanding the issues and risks associated with children's use of digital technologies. Many pupils will access the internet outside school and will need to learn how to evaluate online information and to take care of their own safety and security.

We aim to equip 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.

The purpose of this policy therefore is to:

- Set out the key principles expected of all members of the school community at Central Walker Church of England Primary School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Central Walker Church of England Primary School.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

Roles and Responsibilities

Role	Key Responsibilities
Head Teachers	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements. • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the E-Safety Co-ordinator • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager)

E-Safety Co-ordinator / Designated Child Protection Lead	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
	• Promotes an awareness and commitment to e-safeguarding throughout the school community
	• Ensures that e-safety education is embedded across the curriculum
	• Liaises with school ICT technical staff
	• To communicate regularly with SLT and the designated e-safety Governor/LGC to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• To ensure that an e-safety incident log is kept up to date
	• facilitates training and advice for all staff
	• Liaises with the Local Authority and relevant agencies
	• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

Governors / E-safety governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: • regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs)
Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum

Role	Key Responsibilities
IT Support Service	• To report any e-safety related issues that arises, to the e-safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • that he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • that the use of the *network / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *E-Safety Co-ordinator /Head Teachesr for investigation / action / sanction* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures • To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities. • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws. • E-safety should be discussed at the beginning of every ICT lesson or use of ipad in a lesson.
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • to help the school in the creation/ review of e-safety policies
Parents/carers	• to support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to access the school website in accordance with the relevant school Acceptable Use Agreement. • to consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Teaching and Learning

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use and Central Walker Church of Primary School has a duty to provide pupils with quality internet access.

This policy takes into consideration the recommendations outlined in DfE document; *'Teaching Online Safety in School' June 2019*

How Does Internet Use Benefit Education?

Benefits of using the internet in education include

• access to world-wide educational resources including museums, libraries and art galleries

• rapid and cost effective worldwide communication
• inclusion in the National Education Network which connects all UK schools
• educational and cultural exchanges between pupils worldwide
• access to experts in many fields for pupils and staff
• professional development for staff through access to national developments, educational materials and effective curriculum practice
• collaboration across support services and professional associations
• improved access to technical support including remote management of
• networks and automatic system updates
• exchange of curriculum and administration data with the Local Authority
• access to learning wherever and whenever convenient
• greatly increased skills in Literacy

How Can Internet Use Enhance Learning?

- The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of our pupils
- Children will be taught what internet use is acceptable and what is not and given clear objectives for internet use
- Internet access will be planned to enrich and extend learning activities
- Staff will guide pupils in online activities that will support learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

Good Habits

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

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of E-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the provider including the effective management of content filtering.
- National Education Network standards and specifications.

Dangers to Consider

Some of the dangers children may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyberbullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. The online world develops and changes at great speed. New opportunities, challenges and risks

are appearing all the time. We must demonstrate that we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks.

Underpinning knowledge and behaviours
It is therefore important to focus on the underpinning of knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.

At Central Walker Church of England Primary School this teaching is built into existing lessons across the curriculum, covered within specific online safety lessons and through information sharing events with parents.

Underpinning knowledge and behaviours include:

How to evaluate what they see online
This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

We will help pupils consider questions including:

- 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?

How to recognise techniques used for persuasion
This will enable pupils to recognise the techniques that are often used to persuade or manipulate others.

We will help 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
This will enable pupils to understand what acceptable and unacceptable online behaviour look like. Pupils will learn that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others; and also to recognise unacceptable behaviour in others.

We will help 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; and

- 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
This will enable pupils to identify possible online risks and make informed decisions about how to act. The focus will be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

We will help pupils to identify and manage risk 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.
- 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
This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

We will 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.

Prevent (Read alongside the Anti-Radicalisation policy)

The Counter Terrorism and Security Act 2015 places a duty on schools to prevent people being drawn into terrorism. This duty applies to all schools, whether publicly-funded or independent, and organisations covered by the Early Years Foundation Stage framework.

Children may be exposed to new influences and potentially risky behaviours, influence from peers, influence from older people etc as they begin to explore the internet and social media sites.

The internet creates more opportunities to become radicalised, since it's a worldwide 24/7 medium that allows you to find and meet people who share and will reinforce your opinions.

Schools Leaders must:

- Establish or use existing mechanisms for understanding the risk of extremism
- Ensure staff understand the risk and build capabilities to deal with it
- Communicate and promote the importance of the duty
- Ensure staff implement the duty effectively

Other duties on schools include:

- Effective partnership working with other local agencies, e.g. LSCB, police, health, etc.
- Information sharing
- Maintaining appropriate records
- Assessing local risk of extremism (including Far Right extremism)
- Demonstrating they are protecting children
- Developing clear protocols for visiting speakers
- Safeguarding policies that take account of LSCB policies and procedures
- Training staff to give them knowledge and confidence
- Ensuring there is robust ICT protocols that filter out extremist materials

School buildings must not be used to give a platform to extremists

Channel (Read alongside the Anti-Radicalisation policy)

School staff should understand when it is appropriate to make a referral to the Channel programme. Channel is a programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. It provides a mechanism for schools to make referrals if they are concerned that an individual might be vulnerable to radicalisation. An individual's engagement with the programme is entirely voluntary at all stages.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

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 NEAT Academy can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be recorded and dealt with by a member of the management team, who will decide if sanctions are imposed.
- Any complaints about staff misuse must be referred to the Head Teachers who will decide if sanctions are to be imposed.
- 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.
- The Head Teachers will arrange contact/ discussions with NEAT Academy Newcastle LA and the police to establish clear procedures for handling potentially illegal issues.

- Any complaint about illegal misuse must be referred to the Head Teachers, who will decide if a referral to the police or other relevant authority is necessary, following any guidelines issued by Newcastle Local Authority.
- All staff, pupils and parents will be informed of the complaints procedure.
- All staff, pupils and parents will be informed of the consequences of misusing the Internet and ICT equipment.

Communication

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all classrooms and the ICT suite and discussed with the pupils at the start of each term.
- Pupils will be informed that network and Internet use will be monitored.
- Before each ICT lesson children must be reminded of the importance of e-safety and the responsible use of the internet.
- An e-Safety module will be included in the ICT scheme of work.

Staff and the e-safety policy

- All staff will be given the e-safety policy and its importance explained.
- Every member of staff, whether permanent, temporary or supply, will be informed that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use, both professionally and personally, will be provided, including use of social networking sites such as Facebook.

Enlisting parents' support

- Parent's attention will be drawn to the School e-Safety/Acceptable Use Policy in newsletter, school websites and the school brochure.
- A parents' workshop will be held regularly to inform parents/ carers about e-Safety issues and responsible use.
- Parents will be requested to sign an Acceptable Use agreement as part of the Home School Agreement. (See Acceptable Use policy)
- Information and guidance on e-Safety will be made available to parents/carers in a variety of formats (i.e. weblinks, printed documents, DVD, leaflets, presentations)