Wycliffe Church of England Primary School

E Safety Policy

2022/23

Ratified by the governing body: Jan 2022

To be reviewed on: Jan 2023

Updated: Oct 2022

Vision Statement

We nurture an aspirational family of hard-working, respectful individuals who work collaboratively to have a lifelong love of learning.
"Life in all its fullness" (John 10:10)

> *Our vision is to ensure that our school family are happy and fulfilled in a creative learning environment. This is flexible and caters to individual needs while developing a life-long love for learning through which all members can flourish. We nurture an aspirational family of hard-working, respectful individuals who work collaboratively.*

Background

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

KCSIE 2021 now references four areas of risk online within part two

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism' (KCSIE 2021).

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' (KCSIE 2021).

Conduct: 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' (KCSIE 2021).

Commerce: Commerce – risks such as online gambling, inappropriate advertising, phishing and or financial scams' (KCSIE 2021).

Considering the 4Cs (above) will provide the basis of our online policy.

The use of these new technologies can put young people at risk within and outside the school. Some of the dangers they 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
- cyber-bullying
- access to unsuitable video / internet games/online gambling/scams
- 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. This involves all stakeholders.

The E Safeguarding Committee

- Denise Baxter – E-Safeguarding Leader (Head Teacher, Designated Safeguarding Lead)
- Chris Holdsworth – (Deputy Designated Safeguarding Lead)
- Mirelle Dyson – (ICT Leader)
- Gary Denison - (Named Governor for Child Protection, Governor for E- Safety)

The committee will consult our school technician over technical issues related to safeguarding and security of data.

DSLs should continue to evidence that they have accessed appropriate training and/or support to ensure they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up-to-date information.

Development and Review of this policy.

The E-Safeguarding Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Any developing threats to individuals relating to e-safety will be stored under the E-Safety area of the schools CPOMS and relayed to teachers on a case by case basis dependant on the level of threat posed. Staff training will include e-safety updates termly.

Should serious e-safety incidents take place, the following external persons / agencies could be informed:

- LADO – Local Authority Designated Officer: 01274 435600 or LADO@bradford.gov.uk.
- CSC
- Police

Monitoring the impact of the policy
The school will monitor the impact of the policy using

- logs of reported incidents in the e safeguarding incident log on cpoms
- internal monitoring data for network activity.
- smoothwall is used to filter and monitor content accessed on school computers
- student, staff and parent e-safeguarding data will be gathered through the use of in house e-safeguarding questionnaires annually

Roles and Responsibilities

Governors
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Full Governing Body who will receive regular information about e-safety incidents.
The Governor responsible for child protection has taken on the responsibility for e-Safety.

The role of this Governor will include:

- annual meetings where e-safety issues will be discussed
- annual monitoring of e-safety incident logs
- reporting to relevant Governors through half-termly Safeguarding report
- online safety will be held as a central theme within a whole setting approach to safeguarding, as per the changes to KCSIE 2022.

All staff
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.

All staff should have an awareness of safeguarding issues that can put children at risk of harm. These are examples but it is not an exhaustive list:

- behaviours linked to consensual and non-consensual sharing of nudes and semi nudes images and or videos (also known as sexting or youth produced sexual imagery)
- upskirting, which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm
- initiation/hazing type violence and rituals (this could include activities involving harassment, abuse or humiliation used as a way of initiating a person into a group and may also include an online element)

In all cases, if staff are unsure, they should always speak to the designated safeguarding lead (or deputy).

The Department has produced a one-stop page for teachers on GOV.UK, which can be accessed here: https://www.gov.uk/government/publications/teaching-online-safety-in-schools. This includes teacher training modules on the RSHE topics and non-statutory implementation guidance. The following resources may also help schools and colleges understand and teach about safeguarding:

- DfE advice for schools: teaching online safety in schools
- UK Council for Internet Safety (UKCIS)32 guidance: Education for a connected
- world
- UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people
- the UKCIS external visitors guidance will help schools and colleges to ensure the maximum impact of any online safety sessions delivered by external visitors;
- National Crime Agency's CEOP education programme: https://www.thinkuknow.co.uk/

Headteacher and Senior Leaders

- the headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the e-safeguarding leader
- the headteacher/senior leaders are responsible for ensuring that the e-safeguarding leader and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- the headteacher and e-safeguarding leader are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

Senior leaders must be aware that **information sharing** is vital in identifying and tackling all forms of abuse and neglect, and in promoting children's welfare, including their educational outcomes. Schools and colleges have clear powers to share, hold and use information for these purposes.

E-Safeguarding Leader

- takes day to day responsibility for e-safeguarding issues and has a leading role in establishing and reviewing the school e-safeguarding policy
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- receives reports of e-safety incidents and creates CPOMS log of incidents to inform future e-safety developments,
- reports to child protection governor
- ensure safety is discussed at induction

Technical Staff/ Support

The School Technician ensures:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack

- that they keep up to date with e-safety technical information and update the E-Safeguarding leader as relevant
- that monitoring software (Policy Central) and anti-virus software is implemented and updated

As we migrate to our Digital Strategy we need to remember that technology, and risks and harms related to it, evolve and change rapidly. Schools, the ICT lead, will work alongside them from May 2022 and consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. A free online safety self-review tool for schools can be found via the 360 safe website. https://360safe.org.uk/

Teaching and Support Staff
Are responsible for ensuring that:

- they attend yearly e-safety sessions to ensure they have an up to date awareness of e-safety matters and of the current school e-safety policy
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem to the E-Safeguarding leader for investigation
- digital communications with students / pupils (email/website /voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities.
- students / pupils understand and follow the school e-safety and acceptable use policy
- they are aware of e-safety issues related to the use of mobile phones, cameras, smart watches and hand held devices and that they monitor their use and implement current school policies with regard to these devices

Named person for child protection
They are trained in e-safety issues 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 (see cyber bullying section in this policy)
- peer on peer abuse: to recognise that child on child sexual violence and sexual harassment can occur online

Children
Children are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
Children are expected to report any e-safety incidents they encounter to a member of staff. This information is shared with the children during lessons.
Children must use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Parents / Carers

The school will take every opportunity to help carers / parents to understand issues related to e-safety. We will assist parents to understand key issues in the following ways:

- regular website updates, letters and workshops to parents with the pcso for e-safety provide advice on safe use of the internet and social media at home.
- discussions with parents when e-safety issues have been identified with their child(ren)
- parents are asked to discuss the pupil acceptable use policy with their children and are invited to sign a letter to say they have done so

Community Users

Community Users/visitors and volunteers will inform the Headteacher or Deputy Head of any websites they wish to access. No person can log on to the internet without a user account. A community user account with minimal privileges will be given after discussion of the sites they wish to access.

Education – Pupils

The education of pupils in e-safety is an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

We know that for most people the internet is an integral part of life and has many benefits. We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school but outside as well. We know about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing. As a school community we value all God's children and therefore we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

We will discuss, remind or raise relevant e-safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials. Children and parents need to learn how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
E-Safety education will be provided in the following ways and this may come through our PSCHE curriculum alongside ICT sessions:

- we will provide a curriculum which has E-Safety related lessons embedded throughout but with a planned safeguarding AND e-safety programme is delivered as part of the ICT curriculum
- we will celebrate and promote e-safety through a planned programme of assemblies/worship and whole-school activities, including promoting Safer Internet Day each year
- any internet use will be carefully planned to ensure that it is age-appropriate and supports the learning objective for specific curriculum areas. Parents and children will be

informed as to why social media, some computer games and online gaming, for example, are age restricted.

- pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way
- we will remind pupils about their responsibilities through an acceptable use policy which every pupil will sign and be displayed throughout the school
- school will model safe and responsible behaviour in their own use of technology during lessons
- we will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area and be taught how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- when searching the internet for information, pupils will be guided to use the search engine, https://www.google.co.uk, all use will be monitored and pupils will be reminded of what to do if they come across unsuitable content – Watchguard securely filtering system prevents access to any unsuitable websites.
- pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. All stakeholders need to know that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
- pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline
- key e-safety messages are reinforced as part of a planned programme of assemblies
- children are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information
- children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- children are taught to report any concerns about the materials they are accessing
- we will specifically address online safety, especially with regards to online peer on peer abuse, relationships
- children in ks2 will receive yearly cyber safety workshops from the local police cyber safety unit.
- children will take part in a yearly audit of e-safety and the results will inform future lessons / assemblies.

If children are being asked to learn online at home, for example because of the coronavirus pandemic, schools and colleges should follow the latest advice from the DfE at https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19 (DfE, 2021b).

The NSPCC and PSHE Association also provide helpful advice:

- NSPCC Learning - https://learning.nspcc.org.uk/news/covid/undertaking-remote-teaching-safely
- PSHE - https://pshe-association.org.uk/curriculum-and-resources/search-for-resources

Children should be taught about online safety, including as part of statutory Relationships and Sex Education (RSE), but should recognise that a one size fits all approach may not be appropriate and a more personalised or contextualised approach for more vulnerable children e.g. victims of abuse and SEND, may be needed.

Education - Staff Training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a staff meeting covering e-safety will take place annually; this will be delivered by a member of the e-safeguarding committee.
- a yearly audit of the e-safety training needs of all staff will be carried out with the results informing future training – this will be done by the ICT lead
- all new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies.
- staff will receive updates throughout the year with any new apps/ websites / games that may pose a risk to children via the staff notice board, emails and during staff meetings

Education - Governor Training

Governors must take part in e-safety training / awareness session at induction which is updated regularly. This will be circulated by the BDAT clerking team.

Internet Provision

The school Internet is provided by the Bradford Learning Network, a DofE accredited educational internet service provider. All sites are filtered using the Smoothwall and Watchguard securely filtering system which also generates reports on user activity.

Use of digital and video images - Photographic, Video

- when using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. in particular, they should recognise the risks attached to publishing their own images online
- staff are allowed to take digital / video images to support educational aims. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes
- photographs of children published on the website or (Facebook page) must not contain first and last names. first names are acceptable
- pupils' full names will not be used anywhere on a website or blog
- written permission, in line with current GDPR regulations, will be obtained from parents or carers before photographs of students / pupils are published on the school website and /or social media.

Personal Data Protection

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- do not use USB memory sticks
- sensitive data should not be sent via standard email, instead this should be saved on the school's server or sent using an encrypted email service.

Passwords
All users (adults and young people) will have responsibility for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users and replacement passwords for existing users can be allocated by Mirelle Dyson and OLC – Our Learning Cloud.

Members of staff will be made aware of the school's password policy:
- through the school's e-safety policy and password security policy
- through the acceptable use agreement
- pupils / students will be made aware of the school's password policy in ict and / or e-safety lessons and through the acceptable user agreement

All users (at KS1 and above) will be provided with a username and password by the school's technician who will keep an up to date record of users and their usernames.

Reception will access the school's systems via a shared password. Their access to the internet / system will be closely monitored by the class teachers.

Cyberbullying
Cyberbullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Examples of electronic communication are social networking web sites and apps, texting, use of other mobile or tablet apps, email or online software.

Pupils and adults who feel as if they are being bullied in any way need to talk to someone who they trust. Pupils need to talk to a trusted adult.
Pupils are taught to:
- keep any evidence of cyberbullying by taking screen captures
- make a note about the time and date of any of these messages and any details about the sender
- not forward messages to other people
- not reply to any bullying messages

The school may report serious cyber bullying incidents to the Police.

Social Media

Wycliffe CE Primary uses Twitter under the username @WycliffePrimary and has a Facebook page to promote the learning that takes place within school and to inform parents of on-going events. This takes place with the permission of parents, in line with GDPR to include photographs of the children. Whilst we promote the work of Wycliffe via social media we ensure the anonymity of the children by not publishing full names. Incidents of online feedback and abuse via social media will be dealt with by Denise Baxter or a member of the E-Safety Committee.

Wycliffe has an ONLINE COMMUNICATION AND USE OF TECHNOLOGY section in their Code of Conduct which staff are expected to follow; this policy may be updated more regularly depending on any developing issues regarding social media.

Mobile device policy

Staff

Staff must not use mobile phones and smart watches in lessons. During the school day, mobile phones, smart watches will be switched off or put on 'silent' or 'discreet' mode. Mobile phone use is not permitted during teaching time, while on playground duty and during meetings. In accordance with the Acceptable Use Policy staff should not use personal devices for photography in school. Only School cameras or devices are to be used.

Mobile phones may be used during the school day but only after permission from a member of the Senior Leadership Team. Staff should only use their mobile in the staffroom and our Code of Conduct states that all staff turn off data networks on entry to the building.

Pupils

School does not allow children to bring mobile phones into school until they reach Y6. They are then asked to hand them in on arrival switched off before entering the premises. They are returned by class teachers at the end of the day and can be turned off on exit of the school gates. All mobile phones will be confiscated if found at other times and paretns will be informed.

Pupils are taught about the dangers of using mobile phones, the fact that location services can say exactly where you are and how quickly children can post content online before thinking about the consequences.

School's Mobile Devices

The use of these devices is covered in the pupil and staff Acceptable Use Policies. Pupils know that they must not take pictures of other people without their permission. They are not allowed to download or install apps on any device. These devices are subject to the same levels of internet filtering (Smoothwall) and as are all the school computers accessed by children. Any problems with the device or filtering must be reported a member of the E-Safety team.

E-mail and Internet and Communications systems usage

The following uses of the school's ICT system are prohibited and may amount to gross misconduct and could result in dismissal:

- to make, to gain access to, or for the publication and distribution of inappropriate sexual material, including text and/or images, or other material that would tend to deprave or corrupt those likely to read or see it

- to make, to gain access to, and/or for the publication and distribution of material promoting homophobia or racial or religious hatred
- for the purpose of bullying or harassment, or for or in connection with discrimination or denigration on the grounds of gender, race, religious, disability, age or sexual orientation including HBT language
- for the publication and/or distribution of libellous statements or material which defames or degrades others
- for the publication of material that defames, denigrates or brings into disrepute the school and/or its staff and pupils
- for the publication and distribution of personal data without authorisation, consent or justification
- where the content of the e-mail correspondence is unlawful or in pursuance of an unlawful activity, including unlawful discrimination
- to participate in on-line gambling
- where the use infringes copyright law
- to gain unauthorised access to internal or external computer systems (commonly known as hacking)
- to create or deliberately distribute ICT or communications systems "malware", including viruses, worms, etc.
- to record or monitor telephone or e-mail communications without the express approval of the Governing Body (or the Chair of Governors). In no case will such recording or monitoring be permitted unless it has been established for that such action is in full compliance with all relevant legislation and regulations (see Regulation of Investigatory Powers Act 2000, below)
- to enable or assist others to breach the Governors' expectations as set out in this policy

Additionally, the following uses of school ICT facilities are not permitted and could lead to disciplinary action being taken:

- *for participation in "chain" e-mail correspondence (including forwarding hoax virus warnings)*
- *in pursuance of personal business or financial interests, or political activities (excluding the legitimate activities of recognised trade unions)*
- *to access ICT facilities by using another person's password, or to post anonymous messages or forge e-mail messages using another person's identity*

Use of ICT Equipment
Whilst the school's ICT systems may be used for both work-related and for personal use, the Governing Body expects use of this equipment for any purpose to be appropriate, courteous and consistent with the expectations of the Governing Body at all times.

Policy coverage
This policy covers the use by staff of all school-owned ICT and communications equipment, examples of which include:

- laptop and personal computers
- iPads and other tablet devices

- ICT network facilities
- personal digital organisers and handheld computers
- mobile phones and phone/computing hybrid devices
- on-line storage devices
- image data capture and storage devices including cameras, camera phones and video equipment
- closed circuit television equipment and devices
- lighting and sound equipment and associated devices

This list is not exhaustive.

Use of School ICT Equipment
Any equipment provided to a member of staff is provided for their personal use. Any use of the equipment by family or friends is not permitted and any misuse of the equipment by unauthorised users will be the responsibility of the staff member.

Staff must take reasonable precautions when using school devices outside of school to ensure the protection of the equipment. Irresponsible care and use will be reported to the E-Safety team and/or the Head Teacher.

Laptops must be shut down at the end of every day to ensure that the encryption of the device becomes active. If left in school they must be out of sight.

USB memory sticks are not permitted in school.

Home Learning

T2P:

- using emails to allocate work and receive completed work from children
- feedback given written or verbally
- children can only access the home learning format meaning that they have parental emails log ins and are only able to see their own work and are not able to see other children's names like they usually would in school
- admin (D Baxter and the admin team) are able to access all classes via admin dashboard

Other communication

- monitored year group email for communication between teachers and parents including video conferencing for parents' evening

As guidance from the DfE changes regarding home learning expectations, these strategies may be reviewed and updated to meet the needs of children, families and school.

Whilst it is not possible to cover all eventualities, this policy is published as guidance for staff on the expectations of the Governing Body. Any breaches of this policy or operation of the school's equipment outside statutory legal compliance may be grounds for disciplinary action being taken.