Wycliffe Church of England Primary School

E-Safety Policy

2021/22

Approved by the governing body: January 2021

Date for review: Jan 2022 or when changes are necessary to comply with school policy or national legislation.

Vision Statement

"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 will be flexible and cater to individual needs and develop a love for learning through which all members can flourish. Our priority is to nurture habits and accountability which lead to sustainable development and responsibility.

E-Safety Co-ordinator – D Baxter

ICT Co-ordinator – K Wills/W Cotson

Safeguarding Governor - G Denison

COVID SPECIFIC: During the coronavirus (COVID-19) pandemic, people are relying even more on online technology. Children have been spending more time at home and if they live in an area where there is a lockdown or high level restrictions, they may not be able to see friends and family in person. This makes keeping in touch online extra important.

Many children are spending more time online – and expanding the ways they use the internet. They may join online communities or start using new video-calling platforms. Children who receive support from services may go online to contact social workers, counsellors and others in their support network. While all this can bring benefits to children's mental health and wellbeing, children can be exposed to risk online. Europol has reported an increase in some countries in offenders attempting to contact young people via social media since the outbreak of the virus (Europol, 2020).

Some children may have limited access to the internet at home. This may impact their level and quality of education, their contact with friends and wider family, and potentially affect their mental health.

Specific advice: https://learning.nspcc.org.uk/safeguarding-child-protection/social-media-and-online-safety

During this time rules have been relaxed as staff may need to use devices of their own for filming and uploading lessons for remote learners. They are to be used for these purposes only and NOT for feedback and retrieval of work sent in by families.

KCSinE 2020: *"The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.*

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- ***content:*** *being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;*
- ***contact:*** *being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and*
- ***conduct:*** *personal online behaviour that increases the likelihood of, or causes, harm; for*

example making, sending and receiving explicit images, or online bullying."

New statutory guidance was put on hold in September 2020 due to COVID. This policy contains those updates –although they are not yet statutory – they will become so. These are in red.

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using [name of organisation]'s network and devices
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep children and young people safe by:

- appointing an online safety coordinator: D Baxter – DSL and Headteacher
- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults – codes of conduct and acceptable usage agreements
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others – at home and in school
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents/carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- reviewing and updating the security of our information systems regularly
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse,
- including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual
- exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders
- and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure
- that any problems have been resolved in the long term.

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Child protection
- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff and volunteers
- Anti-bullying policy and procedures
- Photography and image sharing guidance
- Whistleblowing policy
- Behaviour Policy
- Guidance on Safer Working Practice
- Staff code of conduct/staff handbook
- Data Protection
- RSE Policy

The following local/national guidance should also be read in conjunction with this policy and some may form part of a legal framework to support this policy:

- Bradford Education and Safeguarding Team: Guidelines and Procedures (2019)
- PREVENT Strategy HM Government (2019)
- Keeping Children Safe in Education DfE September 2020
- Teaching Online Safety in Schools DfE June 2019
- Working together to Safeguard Children
  - Online abuse: learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- Bullying: learning.nspcc.org.uk/child-abuse-and-neglect/bullying
- Child protection: learning.nspcc.org.uk/child-protection-system

Learning and Teaching

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. 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 provide a curriculum/other lessons which has E-Safety related lessons embedded throughout.

- 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
- 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.
- 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 age-appropriate search engines. all use will be monitored and pupils will be reminded of what to do if they come across unsuitable content
- 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

Staff Training

Our staff receive regular information and training on E-Safety issues, as well as updates as and when new issues arise.

- as part of the induction process all staff receive information and guidance on the E-Safety Policy, the school's Acceptable Use Policy, e-security and reporting procedures

- all staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community
- all staff will be encouraged to incorporate E-Safety activities and awareness within their curriculum areas

Managing ICT Systems and Access (Support Primary T)

- the school will agree on which users should and should not have internet access and the appropriate level of access and supervision they should receive
- all users will sign an Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour whole using the school ICT system and that such activity will be monitored and checked
- at Key Stage 1, pupils will access the network using an individual username and a class password which the teacher supervises. They will ensure that they log out after each session
- at Key Stage 2, pupils will have an individual user account with an appropriate password which will be kept secure. They will ensure that they log out after each session
- all internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times
- members of staff will access the internet using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID or password. They will abide by the school AUP at all times

Managing Filtering

- the school has the Smoothwall filtering system in place which is managed by the school and RM. Banned phrases and websites are identified.
- the school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training/online safety lesson
- if staff or pupils discover an unsuitable site, it must be reported to the E-Safety Co-ordinator immediately
- if users discover a website with potentially illegal content, this should be reported immediately to the E-Safety Co-ordinator. The school will report such incidents to appropriate agencies including Internet Service Provider (ISP), Police, CEOP or the Internet Watch Foundation (IWF)
- any amendments to the school filtering policy or block and allow lists will be checked and assessed by the Headteacher/E-Safety Co-ordinator prior to being released or blocked

- the evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum

E-Mail

- staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked
- staff should not use personal email accounts for professional purposes, especially to exchange any school-related information or documents or to email parents/carers
- staff should not send emails to pupils unless work related and through a school email address
- pupils are encouraged to immediately tell a teacher or trusted adult if they receive any inappropriate or offensive emails
- irrespectively of how pupils or staff access their school email (from home or within school), school policies still apply
- chain messages are not permitted or forwarded on to other school owned email addresses

Social Networking

- staff will not post content or participate in any conversations which will be detrimental to the image of the school. Staff who hold an account should not have parents or pupils as their 'friends'. Doing so will result in disciplinary action or dismissal
- school blogs or social media sites should be password protected and run from the school website with approval from the Senior Leadership Team

Pupils Publishing Content Online

- pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff
- pupils' full names will not be used anywhere on the website, particularly in association with photographs and video
- written permission is obtained from the parents/carers before photographs and videos are published
- any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment
- pupils and staff are not permitted to use their own portable devices to store images/video/sound clips of pupils

Mobile Phones and Devices

General use of personal devices

- mobile phones and personally-owned devices will not be used in any way during lessons or school time. They should be switched off or silent at all times
- no images or videos will be taken on mobile phones or personally owned devices

- in the case of school productions, parents/carers are permitted to take pictures of their child in accordance with school protocols which strongly advise against the publication of such photographs on social networking sites
- the sending of abusive or inappropriate text, picture or video message is forbidden

Pupils' use of personal devices

- pupils in year 6 only who need to bring a mobile phone in to school can do so but this must be handed to the class teacher who will keep it secure until the end of the day
- children must not switch on their mobile phone until off school premises
- pupils who do not follow the school policy relating to the use of mobile phones will not be permitted to bring their mobile phones into school

Screening, Searching and Confiscation

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm
- disrupt teaching
- break school rules
- commit an offence
- cause personal injury
-

Staff use of personal devices

- staff are not permitted to use their own mobile phones or devices for contacting children or their families within or outside of the setting in a professional capacity
- staff will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose
- if a member of staff breaches the school policy then disciplinary action may be taken
- mobile phones and personally -owned devices will be switched off or switched to 'silent' mode, bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods **unless permission has been granted by a member of the senior leadership team in emergency circumstances, eg COVID.** 3&4g must be turned off on the school premises

General Data Protection (GDPR) and E-Safety

Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

DPR is relevant to E-Safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of

personal material.
Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies.
Personal and sensitive information should only be sent by e mail when on a secure network.
Personal data should only be stored on secure devices.
In the event of a data breach, the school will notify the Trust's Data Protection Officer (DPO – P Thompson) immediately, who may need to inform the Information Commissioner's Office (ICO).

Authorising Internet access

- all staff must read and sign the 'Acceptable Use Policy' before using any of school ICT resources
- come September 2020, all parents will be required to sign the home-school agreement prior to their children being granted internet access within school
- all visitors and students will be asked to read and sign the Acceptable User Policy prior to being given internet access within the school
- the school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision

Support for Parents

- parents' attention will be drawn to the school's E-Safety policy and safety advice in newsletters, the school website and E-Safety information workshops
- the school website will be used to provide parents with timely and meaningful information about their children's school lives and work to support the raising of achievement. The website will also provide links to appropriate onlinE-Safety websites

Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Child Protection/Safeguarding Co-ordinator). Regular monitoring and filtering is in place to ensure that access to appropriate material on the internet and key word reporting it in place to ensure safety for all staff and pupils.

Sexual Harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Online sexual harassment is a behaviour which might include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats).

Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified.

Our school follows and adheres to the national guidance - UKCCIS: *Sexting in schools and colleges: Responding to incidents and safeguarding young people*

Responses to Incident of Concern

An important element of E-Safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff, volunteers and pupils have a responsibility to report E-Safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school has incident reporting procedures in place and record incidents of an E-Safety nature on cpoms.

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or expulsion, in accordance with the school's Behaviour or Discipline Policy. The school also reserves the right to report any illegal activities to the appropriate authorities.