Wycliffe Church of England Primary School

E Safety Policy

2023/2024

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.*

Contents

BDAT Policy Statement

Bradford Diocesan Academies Trust (BDAT) regards knowing how to stay safe online as integral to the development and safeguarding of our pupils. We are committed to developing a culture where pupils are aware of the risks they face online and know how to keep themselves safe, but where they can also harness the opportunities within the digital world to enhance their education.

We aim to ensure our schools:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate any online safety incidents, where appropriate

As part of our focus on diversity and inclusion, BDAT pledges that our policies will seek to promote equality, fairness, and respect for all staff and pupils. Our policies reflect the BDAT values of inclusion, compassion, aspiration, resilience, and excellence. By working closely with a range of stakeholders, such as our school, union, and HR colleagues, we have ensured that BDAT's policies do not unlawfully discriminate against anybody.

This policy should be read in conjunction with the school-specific behaviour policy, the safeguarding policy, the anti-bullying policy and the equality policy. It will be reviewed annually in order to assess its implementation and effectiveness.

Introduction and Aims

Information and Communications Technology (ICT) in the 21st Century is seen as an essential resource to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. New technologies have become integral in today's society, both within schools and 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 and, consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies staff, children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Making /receiving phone calls via their mobile phones
- Other mobile devices with web functionality

- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

This online safety policy recognises the commitment of Wycliffe Primary School to online safety and acknowledges its part in the school's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. 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.

We believe the whole school community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The online safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities.

Keeping Children Safe In Education 2022 references four areas of risk online within part two, these being:

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

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

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

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams

As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision that we build our 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.

Roles and Responsibilities

The Governing Body

The governing body has overall responsibility for monitoring this policy, holding the Head Teacher to account for its implementation and reviewing its effectiveness.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL). The governor who oversees online safety is G Denison.

All governors will:

- Ensure that they have read and understand this policy
- Ensure that online safety is a running and interrelated theme while monitoring the whole school approach to safeguarding
- Support the work of Wycliffe Primary School in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety awareness
- Have an overview of how the school IT infrastructure provides safe access to the internet and the steps Wycliffe Primary School takes to protect personal and sensitive data
- Ensure appropriate funding and resources are available for Lightcliffe Academy to implement their online safety strategy

The Head Teacher

The Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout Wycliffe Primary School. They will:

- Liaise with the Governors to ensure they are provided with relevant online safety information
- Develop and promote an online safety culture within the school community
- Ensure that all staff receive suitable CPD to enable them to carry out their roles in relation to online safety
- Ensure that all staff, pupils and other users agree to the ICT Acceptable Use Policy and that new staff have online safety included as part of their induction procedures
- Receive and regularly review online safety incident logs; ensuring that the correct procedures are followed should an online safety incident occur in school and review incidents to see if further action is required

The Designated Safeguarding Lead

The details of Wycliffe Primary School's DSL and deputies are set out in our safeguarding policy as well as in relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout Wycliffe Primary School.
- Working with the Head Teacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the Wycliffe Primary School policy
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school anti-bullying policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head Teacher and Local Governing Body

IT Staff

The BDAT Head of Corporate Projects is responsible for managing and overseeing the Trust-wide ICT Managed Service Provision, which includes the following:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online whilst at school, including terrorist and extremist material

- Ensuring that Wycliffe Primary School's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting security checks and monitoring Wycliffe Primary School's ICT systems on an ongoing basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Support Wycliffe Primary School in providing a safe technical infrastructure to support learning and teaching
- Ensuring appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information and reviewing these regularly to ensure they are up to date
- Ensuring that provision exists for misuse and malicious attack detection
- Ensuring that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management
- Ensuring that suitable access arrangements are in place for any external users of Wycliffe Primary School's ICT equipment
- Ensuring appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

All Staff and Volunteers

All staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of Wycliffe Primary School's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Working with the school staff to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Wycliffe Primary School's anti-bullying policy
- Taking responsibility for ensuring the safety of sensitive school data and information
- Developing and maintaining an awareness of current online safety issues, legislation and guidance relevant to their work
- Maintaining a professional level of conduct in their personal use of technology at all times
- Ensuring that all digital communication with pupils is on a professional level and only through school based systems, NEVER through personal email, text, mobile phone social network or other online medium.
- Embedding online safety messages in learning activities where appropriate
- Supervising pupils carefully when engaged in learning activities involving technology
- Ensuring that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Parents

Parents are expected to:

- Ensure their child has read, understood and agreed to the terms on acceptable use of ' Wycliffe Primary School's ICT systems and internet

- Help and support the school in promoting online safety
- Discuss online safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with Wycliffe Primary School if they have any concerns about their child's use of technology
- Support the school's approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? - UK Safer Internet Centre
Hot topics - Childnet International
Parent factsheet - Childnet International
Healthy relationships – Disrespect Nobody
Safer Internet Day 2023 - film for parents and carers - YouTube
Online Safety Basics - National Cybersecurity Alliance (staysafeonline.org)
https://parentzone.org.uk/
TALK Checklist by Internet Watch Foundation | Home (iwf.org.uk)

Pupils
Pupils are expected to:

- Take responsibility for their own and each other's' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights and values of other pupils in their use of technology at school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all online safety incidents to appropriate members of staff in school
- Discuss online safety issues with family and friends in an open and honest way
- Know, understand and follow school policies on the use of technology
- Know, understand and follow school policies regarding bullying
- Support the school's approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

Visitors and Members of the Community
Visitors and members of the community who use Wycliffe Primary School's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum. This will be done through:
- An age appropriate curriculum which has online safety related lessons embedded throughout but with a planned online safety programme as part of the ICT and PSHE curriculum
- Celebration and promotion of online safety through collective worship and whole-school activities, including Safer Internet Day each year

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In Key Stage 2, pupils will be taught to:

- Use technology safely, respectfully and responsibly, keeping personal information private
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Educating Parents about Online Safety

Wycliffe Primary School will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. We will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL or a member of the safeguarding team.

Cyber-Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group.

Cyber bullying includes sending abusive or hurtful texts, emails, social media posts, images or videos, deliberately excluding others online, spreading nasty gossip or rumours online and imitating others online or using their log-in.

Cyber bullying can be overt or covert but uses digital technologies, including hardware such as computers and smartphones, and software such as social media, instant messaging, texts, websites and other online platforms. Cyber bullying can happen at any time, can be in public or in private online spaces and so is sometimes only known to the target and the person bullying.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Wycliffe Primary School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, we will follow the processes set out in the anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

The Head Teacher, and any member of staff authorised to do so by them (including the DSL, senior leaders and the pastoral team), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Head Teacher or Designated Safeguarding Lead
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil’s cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a ‘good reason’ to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Head Teacher, Designated Safeguarding Lead or another member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable Use of the Internet in School

All pupils, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet.

Visitors will be expected to read and agree to Wycliffe Primary School's terms on acceptable use if relevant. Use of Wycliffe Primary School's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the ICT acceptable use agreement.

Pupils Using Mobile Devices in School

Only Year 6 pupils may bring mobile devices into school. They are not permitted to use them whilst on school site. They should be switched off before entering the playground and handed to a class teacher on arrival. They will be returned at 15.15 and can be turned back on once out of the playground.

Any use of mobile devices in school by pupils must be in line with the ICT acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

BDAT ensures that all laptops provided for use inside and outside school have:

- Anti-virus and anti-spyware software installed
- Up-to-date operating systems with the latest updates installed

Staff members must not use the device in any way which would violate Wycliffe Primary School's ICT terms of acceptable use. Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from a member of IT support.

Responding to Issues of Misuse

Where a pupil misuses Wycliffe Primary School's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses Wycliffe primary School's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

Wycliffe Primary School considers whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

IT Systems

Wycliffe Primary School decides which users should and should not have internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in school and will be responsible 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. Pupils are taught about safe practice in the use of their log in and passwords.

Staff are also given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorized users only, with proper procedures being followed for authorizing and protecting login and password information.

Our practice in relation to passwords is as follows:

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system).
- We provide all staff with a unique, individually named user account and password for access to IT equipment, email and information systems available within school.
- All pupils in KS1 and above have a unique, individually named user account and password for access to IT equipment and information systems available within school. Reception class access the school systems via a shared password.
- All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.
- We maintain a log of all accesses by users and of their activities while using the system in order to track any online safety incidents. Class teachers closely monitor the use of the internet by pupils in school.
- Passwords must be difficult to guess and should be a mixture of upper case and lowercase, numbers and symbols.
- Staff and pupils will have to reset their passwords at given intervals.

Using the Internet and Email

We provide the internet to:

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance Wycliffe Primary School’s management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the examination boards and others

Email is regarded as an essential means of communication and Wycliffe Primary School provides all members of the school community with an e-mail account for school-based communication.

Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained.

All email activity is recorded in line with data protection laws. The school is able to view these records in situations where this is called upon.

As part of the curriculum pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.

Wycliffe Primary School will set clear guidelines about when pupil-staff communication via email is acceptable and staff will set clear boundaries for pupils. Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email address.

Responsible use of personal web mail accounts on school systems is permitted for staff only outside teaching hours.

Publishing Content Online

Wycliffe Primary School maintains editorial responsibility for any school-initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. We maintain the integrity of the school website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.
The point of contact on the web site is the school address, e-mail and telephone number.

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by pupils, governors and staff in a social context which is considered to bring Wycliffe Primary School into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

We recognize that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Identities of pupils are protected at all times and, in line with GDPR regulations, parents have the option to opt out so that photographs of individual pupils are not published on the website without permission. Group photographs do not have a name list attached.

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

We are happy for parents to take photographs at school events, except in specific circumstances where rights holders refuse permission, but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own they should not be uploaded to social media sites and can be only used for their personal use.

Further information can be found in the linked policies detailed below.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and safeguarding team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our safeguarding policy.

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPOMS, as per the Safeguarding Policy. Should serious online safety incidents take place, the following external persons/agencies could be informed:

- LADO – Local Authority Designated Officer
- Children's Social Care
- Police

This policy will be reviewed every year by the Head Teacher and ratified by the Local Governing Body. Given the ever-changing nature of technology, we will ensure that this review is supported by ongoing risk assessment which reflects current online safety issues that children face.

We will monitor the impact of the policy using:

- Logs of reported incidents in the online safety category on CPOMS
- Internal monitoring data for network activity gathered through filtering and monitoring software
- Pupil, staff and parent voice

The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links to Legislation, Guidance and Other Policies

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation
- Protecting children from radicalisation

It reflects existing legislation, including but not limited to The Malicious Communications Act 1988, the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study and complies with our funding agreement and articles of association.

This policy also links with a number of other policies, including:

- BDAT MAT Behaviour Statement
- Wycliffe Primary School's Behaviour Policy
- Suspensions and Exclusions Policy
- Complaints Policy
- Safeguarding and Child Protection Policy
- Equality and Diversity Policy
- Preventing Radicalisation Policy
- Acceptable Use of IT Policy
- Use of ICT for Communications and Teaching Policy
- Social Media Policy
- Staff Code of Conduct
- Staff Disciplinary Policy and Procedure
- GDPR Policy

Appendix 1:

Acceptable Use of ICT Agreement for Staff – Sept 2022

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Denise Baxter, Headteacher or Fiona Cressey, Business Manager.

- I will only use the school’s email / Internet and any related technologies for professional purposes or for uses deemed ‘reasonable’ by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role and in line with the staff code of conduct
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils in line with the staff code of conduct.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not use or install any hardware (including USB sticks) or software without permission from the e-safety co-ordinators.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school’s e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not use self purchased technology to store any sensitive/GDPR material such as data, photos etc

- I understand that only I can use the school laptop assigned to me

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ……..……………………………… Date ……………………

Full Name ……………………………………... (printed)

Job title: ………………………………………………………………..