The Willows Catholic Primary School

Online Safety Policy

Updated: Spring 2024

Contents

1. Introduction

At The Willows Catholic Primary School, we see technology as a vital area of development in all subjects and make significant steps to ensure that all staff and children have access to relevant, high quality technology. In many areas of work, the use of technology is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the technology systems and data are maintained at a level that is appropriate for our needs. Online safety is a fundamental part of all areas of Computing and, at The Willows, it is a priority across all areas of the school.
The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

2. Intent

With the great speed at which technology that accesses the internet is easily available in the forms of mobile phones, tablets, games consoles and smart TVs, it is imperative that all children, parents/carers, staff and governors at The Willows understand the benefits and dangers of using these devices. As the use of technology is an integral part of the teaching and learning, we view the teaching of online safety as a fundamental part of our curriculum. At every opportunity, online safety is taught and discussed with our children where appropriate to everyday use, as well as having a specific focus on relevant areas of online safety, for example, where there are issues identified involving our children, in the media, on Safer Internet Day and where there are concerns over common recurring issues.

We aim to support the education and implementation of online safety with our parents/carers through providing links to relevant websites accessed through our school website; a weekly section of online advice sent to both children and parents/carers via our app; the Online Safety Policy being available from our website; and asking children and parents/carers to read and sign relevant information in our Acceptable Use Policy, reviewed annually.

The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using technology. In delivering the curriculum, teachers plan for and make use of this, for example, web-based resources and e-mail. Access to life-long learning and employment increasingly requires computer and communications use and pupils are taught to develop these skills efficiently. Access to the internet is a necessary tool for staff and pupils. It is an entitlement for pupils who show a responsible and mature approach towards its use.

We ensure that children and staff at The Willows are protected in their use of technology through encouraging and modeling appropriate use, for example, during staff meetings or lessons, being supervised and having appropriate restrictions and filters in place.

Knowledge of what to do when problems occur is also a priority for our school and this is delivered effectively through staff meetings and instilling sound knowledge in all children during lessons.

Computing and the related technologies such as e-mail, the internet and mobile devices are an integral part of our daily life in school and we therefore strive to give pupils and staff the opportunities to:

- Access world-wide educational resources
- Participate in new initiatives
- Gather information and have cultural exchanges between appropriate staff and pupils in other schools
- Participate in staff discussions with experts in many fields
- Provide access to educational materials and good curriculum practice
- Communicate with the advisory and support services, professional associations and colleagues
- Have access to and become skilled in the use of emerging technologies
- Carry out all of the above safely and responsibly.

3. Roles and Responsibilities

The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance
- Ensuring the DSL's remit covers online safety
- Reviewing this policy on an annual basis
- Ensuring their own knowledge of online safety issues is up-to-date
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction
- Ensuring that there are appropriate filtering and monitoring systems in place
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

Mrs. Barnett, the Headteacher, has the role of DSL (Designated Safeguard Lead), with the support of Mr. Wylde and Mr. Knight, and any problems, worries or concerns must be reported to her as soon as possible. If Mrs. Barnett is not available, the next person to report to is Mr. Wylde (Deputy DSL). It should be noted that sharing/viewing illegal information/images with others is a criminal offence; however it may be necessary to inform/show Mrs. Barnett in her role of DSL to enable her to take further action if necessary and this may involve contacting the police or getting support from an organisation such as the Child Exploitation and Online Protection Centre (CEOP).

The role of the DSL includes:

- Having overall responsibility for ensuring the development, maintenance and review of the school's online safety Policy and associated documents, including Acceptable Use Policies, supported by Mr. Wylde and Mr. Knight
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored and that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding
- Ensuring that all staff are aware of reporting procedures and requirements should an online safety incident occur
- Ensuring an online safety Incident Log is appropriately maintained and regularly reviewed audited and evaluated
- Keeping personally up-to-date with online safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the CEOP
- Providing or arranging online safety advice/training for staff, parents/carers and governors, including induction and safeguarding training
- Ensuring that SLT, staff, technicians, children and governors are updated as necessary
- Liaising closely with the other officials such as the Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.

All staff members are responsible for:

- Taking responsibility for the security of digital systems and electronic data they use or have access to
- Modelling good online behaviours
- Maintaining a professional level of conduct in their personal use of technology
- Having an awareness of online safety issues
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online
- Reporting concerns in line with the school's reporting procedure
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Handling online safety concerns

- Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy
- Concerns regarding a staff member's online behaviour are reported to the DSL, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct. If the concern is about the headteacher, it is reported to the Chair of Governors.
- Concerns regarding a pupil's online behaviour are reported to the DSL (Mrs. Barnett), who investigates concerns with relevant staff members, e.g. technicians, and manages

concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy
- Where there is a concern that illegal activity has taken place, the DSL contacts the police
- The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy
- All online safety incidents and the school's response are recorded by the DSL.

Pupils are responsible for:
- Adhering to the Acceptable Use Agreement and other relevant teaching
- Seeking help from school staff if they are concerned about something they or a peer have experienced online
- Reporting online safety incidents and concerns in line with the procedures within their Acceptable Use Policy.

4. Areas of concern

Cyberbullying

Cyberbullying can include the following:
- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Peer-on-peer sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff understand that this abuse can occur both in and outside of school and off and online, and remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff are aware of:
- Threatening, facilitating or encouraging sexual violence

- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery.

Staff are aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff are aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL ensures that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met
- Having money or new possessions, e.g. clothes and technological devices that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they bring these concerns to the DSL without delay, who handles the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members are aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they report this to the DSL without delay, who handles the situation in line with the Prevent Duty Policy.

Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff are aware that online activity both in and outside of school can have a substantial impact on a pupil’s mental state, both positively and negatively. The DSL ensures that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

Concerns about the mental health of a pupil are dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they report it to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes
- Careful to avoid needlessly scaring or distressing pupils
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils
- Proportional to the actual or perceived risk
- Helpful to the pupils who are, or are perceived to be, at risk
- Appropriate for the relevant pupils' age and developmental stage
- Supportive
- In line with the Child Protection and Safeguarding Policy

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school factors into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL considers a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL ensures that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

5. Security and Data Management

Security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment.

In line with the requirements of the Data Protection Act (1998) and GDPR (2018), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data is:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection
- Kept secure and staff are informed of what they can or can't do with data through this online safety Policy and the Acceptable Use Policy (AUP)
- Accessed by relevant staff who know the location of data or are aware of who to ask
- Only used via approved means to access, store and dispose of confidential data

- Not accessible without passwords
- Backed up using a system that is overseen by our technician
- Backed up and secured via own class teachers such as reports, planning and assessment, etc.

Staff are reminded about security through staff meetings and in the Acceptable Use Policy.

6. Use of Mobile Devices

Any personal device that is brought into school is the responsibility of the user.
Personal devices are not permitted to be used in any toilets.

The EYFS framework: Section 3.4 (2012) states that
"....Safeguarding policy and procedures must include an explanation of the action to be taken in the event of an allegation being made against a member of staff, and cover the use of mobile phones and cameras in the setting."

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- iPads

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.
Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Mobile phones

Staff

All staff are allowed to bring in a mobile phone for personal use. During school session times, all phones should be set to silent mode and kept away out of sight. They must stay away during all of the school sessions throughout the day. Special permission may be sought and sanctioned by Mrs. Barnett (the Headteacher) in certain circumstances, for example, during pregnancy, illness or possible medical emergencies. There are clear notices around school and in the staffroom about keeping phones away.
Phones may be used during break times, out of the sight and hearing distance of children. Designated areas are the staffroom or the office (if it is available).
Personal devices **must not** be taken into EYFS under any circumstances and there are clear notices on the doors leading into those areas.
Personal devices **must not** be used to take photos or videos of any pupils.
For security reasons, staff have access to a lockable locker if required and should speak to Mrs. Barnes to arrange this.
Staff are not allowed to connect any of their personal devices to the school's Wi-Fi network or server.
Staff report any concerns over staff use of personal devices to the DSL.

Parents

Parents are politely requested to leave their phone out of sight and refrain from answering any phone calls or using text messaging whilst inside the school building. They are also politely asked to show consideration to other parents and children whilst on school property. There are clear signs around school requesting this.

Activities outside the normal school day. (Sports day, shows, PTFA events)

Parents are asked to set their phone to silent mode during any events and to show consideration to parents and children whilst on school property.
Photographs and video footage can be taken of their own child under the Data Protection Act (1998), the as long as it is only of their child and for their personal viewing only. Parents are reminded that they should not post photographs or video footage of other children without their prior consent on social media sites at every event.

*Under the Data Protection Act (1998), parents are entitled to take photographs of **their own** children on the provision that the images are for **their own** use, e.g. at a school production. Including other children or for another purpose could constitute a potential breach of Data Protection legislation. (Lancashire County Council)*

Parents are not permitted to use any technologies that belong to the school.

Children

Children are not permitted to bring mobile devices to school. There are certain circumstances where children may be required to bring a mobile phone to school, for example, emergency reasons - if they travel to school by themselves and permission is sought from the Headteacher before this happens. If a mobile phone is brought to school for any reason, it is handed in to the office as soon as the child arrives at school and is collected from the office at the end of the day. During a pandemic, such as Covid-19, devices are placed by the child in a closed plastic wallet and kept out of reach of the children in the child's classroom.
Children are not allowed to take videos or photographs using their mobile devices on school property. If this does happen it is reported to the DSL as soon as possible.

Other mobile devices including tablets, Smart Watches and Fitbits

Staff

Staff are allowed to bring in other mobile devices, for example tablets, smart watches and Fitbits, as long as they abide by this Online Safety Policy and the Acceptable Use Policy and are reminded here that they must not be linked to the school's server or Wi-Fi network and they must not be used to take photographs or video footage of children for any reason.

Staff have been provided with an iPad that they can use to read and send email, take the register, photograph children for the website or Seesaw and do other work related tasks.

Parents

The same rules that apply to mobile phones also apply to other mobile devices.

Children

Children are not permitted to bring in other devices such as smart watches and Fitbits, due to being able to make and received calls, take photographs and video. If a device is brought to school for any reason, it is handed in to the office as soon as the child arrives at school and is collected from the office at the end of the day. During a pandemic, such as Covid-19, devices are placed by the child in a closed plastic wallet and kept out of reach of the children in the child's classroom.

Children are not allowed to take videos or photographs using their mobile devices on school property. If this does happen it is reported to the DSL as soon as possible.

School

Each teacher has been specifically allocated an iPad, as well as other relevant members of staff. There are restrictions in place and the devices are monitored and access the internet through filtering systems.

Staff are aware that they should follow guidance in this document and the Acceptable Use Policy, with special regards to using a passcode that nobody else knows and not leaving the device lying around for others to access.

Content is downloaded through the official iPad app store using the head's account.

School also has 30 iPads for whole school use that are stored in a trolley in the juniors. A timetable is located on the trolley to book out and monitor their use. They have been set up with appropriate restrictions such as no access to email or Facetime. During a pandemic, such as Covid-19, devices are thoroughly sanitised after each use and before being put away.

School also has two trolleys, each with 15 iPads in set up in the same way.

Some classes have a set of iPads or laptops for their specific class use. Again these are setup and used in line with this policy and the Acceptable Use Policy.

School has 32 laptops that are leased from Stone and Freedom tech.

7. Use of Digital Media
(Cameras and recording devices)

Consent and Purpose

Written consent for taking and using images in school, on the website and for media purposes is sought at the start of every school year and adhered to by everyone. Written consent details are kept in a separate permission document in each individual class. Consent is split into sections to ensure clarity of what is being agreed to – photographs being taken and used on the website and photographs for any newspaper/media articles. Staff have a record of this information and use it appropriately.

Taking Photographs / Video

All classes have access to a device with a camera (mostly through iPads) with still and video capabilities and the class teacher and TAs connected to that class may use the device for educational/school purposes.
Children have access to cameras through use of the iPads and may do so with permission, for educational purposes. Children can upload their work, with permission, to their Seesaw journal.
Staff and children are reminded to remove any images as soon as they have been used.
There is a dedicated area on the server for staff to put photos and video as a record of our schools' achievements and also for the end of Year 6 video.
Mrs. Barnett has a more professional camera that may be used if a more professional finish is required, for example, for the website or a brochure of some sort.
The use of personal recording devices is not permitted. If anyone is seen using their own devices they are reminded of the rules in this document and it is reported to the DSL as soon as possible so that she can respond to the situation.
Children/staff may refuse to be part of a photograph/video, even if permission has been given by a parent/carer and their individual rights must be respected.
Care should be taken when videoing/taking photos of children/staff to ensure that they are not put in compromising situations, for example, distressed, injured or in context that could be embarrassing or misinterpreted. Care is also needed to ensure that children are appropriately dressed and represent the school and themselves in the best possible light.
Staff check each individual photo that is being used for a purpose to ensure that no-one is in a compromising position, especially any children or staff in the background.
Care is taken to ensure that certain children are not seen as favourites for any images/video used on the website or around school.
Any toilet area is strictly off limits for any recording devices, as is any swimming baths and changing areas and any similar area when on residential. Mobile phones taken to the swimming baths must remain in the staff's pocket at all times whilst on site. Recording devices must not be out in school whilst children are getting changed for any reason and photos/videos of children getting changed are strictly forbidden.

Photographs/video of children showing a background context, piece of work or in a group situation are preferable.

Storage of Photographs / Video

Class recording devices have a passcode to prevent children and other adults from accessing the images.

Any photographs/video footage of children are stored on a password protected laptop/computer. Memory sticks are not to be used in our school.

Teaching staff and TAs have permission to access photographs/videos for school purposes.

Should an image/video be required to be taken out of the school environment, this is very unlikely, any appropriate details of what is happening and why will be discussed with Mrs. Barnett and any other appropriate adults/parents/carers and permission from Mrs. Barnett should be sought.

Photographs/video footage, assessment data and other confidential documents (IEPs) MUST NOT be sent via email.

Staff do not store any images or video on their personal devices. Permission is granted for the person who is involved in making the Leavers DVD to store images/video footage until the DVD is complete. Images/video are then immediately removed from any devices.

In the summer term, any photographs or video footage is put on the designated photo area on the server and any photographs/video footage are deleted from the class devices. (This is reminded to staff at the end of a school year.)

Publication of Photographs / Videos

Consent must have been given before a child's photograph/video footage is published to the school's website and it is the responsibility of the member of staff to make sure that permission has been given for all children and staff in the photograph – this is found in the permission document.

Names must not accompany any photographs or video footage without the correct consent.

Written consent for taking and using images in school, on the website and for media purposes are sought just after the start of every school year and adhered to by everyone. Written consent details are kept in the office and staff are made aware of any issues/restrictions at the start of the school year or when a new child arrives.

When publishing images.

Through staff meetings and online safety meetings, staff are reminded that:

- Children's images are not to be displayed on unofficial sites e.g. Social Media Sites.
- Full names and personal details will not be used on any digital media, particularly in association with photographs.
- There are risks associated with publishing images, particularly in relation to use of personal Social Network sites.

- They ensure that personal profiles are secured and do not display content that is detrimental to their own professional status or could bring the school into disrepute.

Video Conferencing, VOIP and Webcams

Occasionally, video conferencing can enhance the curriculum and staff discuss any issues concerning online safety.
When using webcams, it is important to remember that the images which are broadcast from school could be captured as a snapshot or video clip from a system receiving the broadcast and therefore permissions need to be checked.
During a pandemic such as Covid-19, Microsoft Teams is used so that staff can communicate in a safe way. Online safety procedures are carried out.

8. Communication Technologies

New technologies are risk assessed against the potential benefits to learning and teaching before being employed throughout the school. As new technologies are introduced, this Online Safety Policy is updated and all users are made aware of any changes.

Online Homework – Seesaw

Homework is set online through the app/website Seesaw. Activities are appropriately chosen by the teacher to build on learning that has taken place throughout the week. Staff ensure that children have access to Seesaw and provide an appropriate alternative if they do not. Work is also added to the child's Seesaw journal where appropriate. It is also used as a way of communication between staff and parents/carers.

Email

Staff

All staff have access to an approved school email account and can only use these accounts for school purposes.
Where staff need to contact parents/carers, they must use the Willows app, ensuring that the language that they use is standard English that cannot be misinterpreted. Use of text or slang language is not used in communication to parents/carers.
Personal email accounts are not used during school hours or on school equipment unless individual permission had been granted from Mrs. Barnett, the Headteacher.
Staff do not enter into email or text communications with children apart from helping with homework or explaining next steps on Seesaw.
Staff are made aware of the dangers of opening emails that are classified as spam and are educated in good online safety in this area.

Staff are reminded (Acceptable Use Policy) that email communications may be monitored at any time.
Staff should report any inappropriate emails to the DSL as soon as possible and delete any spam or phishing emails.
Staff are aware that they should not open any suspicious emails or attachments that appear to be inappropriate as doing so may mean that they commit a criminal offence or cause harm to the school's system.

Staff are made aware that email is covered by The Data Protection Act (2018) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

Children

Email accounts for children are set up through Purple Mash ensuring that children cannot be identified from their email address. Children can email each other, but do not have open access to send or receive emails.
Online safety is adhered to ensuring that children do not give any personal details and that a member of staff checks the content of any emails before they are sent. This is made clear before any emails are sent or received, through online safety lessons.
Subject/email address/content of received emails is monitored by a member of staff to ensure that children are not exposed to anything inappropriate.
Children report anything inappropriate/unexpected to the member of staff immediately.
Staff must report anything inappropriate/unexpected to Mrs. Barnett.

Social Networks

Our school has a Facebook page, but it is not used.

Staff are asked to follow the guidelines given by Lancashire on their use of social network sites:

Social Network sites allow users to be part of a virtual community. Current popular examples of these sites are Facebook, Twitter, Club Penguin and Moshi Monsters (for children). These sites provide users with simple tools to create a profile or page including basic information about themselves, photographs, and possibly a blog or comments. As a user on a Social Network site, you may have access to view other users' content, send messages and leave unmediated comments. Many Social Network sites are blocked by default through filtering systems used in our school, but these settings can be changed at the discretion of Mrs. Barnett, the Headteacher
(See ***http://www.lancsngfl.ac.uk/lgfladvice/index.php*** *for more details).*
Although use of Social Networks tends towards a personal basis outside of the school environment, their use as a tool for communicating with parents is becoming more commonplace in primary schools.

If a school Social Network page is to be created, you must consider the purpose and audience and also ensure that the privacy settings and interaction are appropriate.
Remember; whatever methods of communication are used, individuals should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and potentially remains there forever.

All staff are made aware of the following points:

- The content on Social Network sites may be unmediated and inappropriate for certain audiences
- If a Social Network site is used personally, details are not shared with children and privacy settings are reviewed regularly to ensure information is not shared automatically with a wider audience than intended (see Mrs. Barnett or Mr. Knight for support in this area.)
- They do not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites
- Any content posted online does not:
    - bring the school into disrepute.
    - lead to valid parental complaints.
    - be deemed as derogatory towards the school and/or its employees.
    - be deemed as derogatory towards pupils and/or parents and carers.
    - bring into question their appropriateness to work with children and young people.
- Staff do not communicate with children using any digital technology, other than Seesaw, especially where the content of the communication may be considered inappropriate or misinterpreted. Online Communications with parents, past pupils or siblings of pupils, especially if under the age of 18, is discouraged
- Children, including, past pupils, are not added as 'friends' on any Social Network site
- Staff do not post inappropriate comments about staff or children that could be construed as instances of cyberbullying
- Staff do not post images of children or adults on profiles without permission of the individuals involved, especially if the photographs contain children other than their own
- Staff receive annual training on how to use social media safely and responsibly. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media. Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are friends with a parent at the school, they will disclose this to the DSL and will ensure that their social media conduct relating to that parent is appropriate for their position in the school
- Pupils are taught how to use social media safely and responsibly through the online safety curriculum
- Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behavioural Policy.

Instant Messaging or VOIP (Voice Over Internet Protocol)

These are all blocked through restrictions on the iPad or the Lancashire filter.
Staff are made aware of the risks involved in using this technology, for example, viewing inappropriate images or making unsuitable contacts, through online safety meetings.
Staff who bring iPads/tablets in for personal use do not to connect to the school server or Wi-Fi for any reason. They are not to use personal email/facetime during session hours and if they are used at break time they should adhere to the times and places mentioned previously in the Mobile phone section.
Staff do not to use school iPads for any personal communications.
Parents are contacted through the Willows app. This allows both forms to be completed and is also a messaging system. It is requested that any emails, where appropriate, are sent to Mrs. Barnes in case any parent/carer phones with any questions or concerns. It is advisable that the content is discussed with Mrs. Barnett before being sent.

Websites and other online publications

Our school website effectively communicates online safety to parents/carers through links to the Thinkuknow website, Vodaphone online and magazine and Childline website. Also through displaying the Online Safety Policy online, suggesting reading material, for example, the digital parenting website, sending home copies of the Vodaphone Digital Parenting magazine and providing support through Parent evenings on online safety. We also send home weekly advice to children and parents/carers on a wide range of relevant topics.
Only relevant staff have the ability to update information on the website and regular meetings/discussions take place to ensure guidance is adhered to.
Overall responsibility for the website belongs to Mrs. Barnett, but responsibility for appropriate areas is delegated to relevant teaching staff.
Copyright is strictly adhered to and discussed with children as part of their online safety education.
Names and details are not used on the website and, at present there is a password protected area for the Governors to access.
Any downloadable material is converted to the read-only format of PDF, where possible, to prevent content being manipulated and potentially redistributed without the school's consent.

9. Remote Learning

All remote learning is delivered in line with the school's Pupil Remote Learning Policy.
The school carries out risk assessments for the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. We consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

We ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required. During the period of remote learning, we maintain regular contact with parents to:

- Reinforce the importance of children staying safe online
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites
- Direct parents to useful resources to help them keep their children safe online.

School is not responsible for providing access to the internet off the school premises and will is not responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.
We do however give technical support and advice in setting up devices.

10. Infrastructure and Technology

Our school ensures that the infrastructure/network is as safe and secure as possible.
It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service.
Anti-Virus software is on devices and is configured to receive regular updates.

Children's access

Children are supervised by a member of staff at all times when using computers/laptops/iPad/other devices in school.
Each child has a specific login with a password for the different websites that school subscribes to.
Computers/laptops are set up with the same format to ensure consistency for all.
Children cannot access any areas deemed not appropriate for example, administrator tools, due to password usage.

Adult access

Staff can access areas deemed appropriate for their use and have access to the appropriate password.

Passwords

Staff can access the school server through the teacher login and are reminded that care is needed when typing this in when children or other adults are nearby. They should also ensure

that the password is not given to others, especially written down, particularly supply teachers.
There is a specific account that has been set up for supply teachers.
The administrator's password/installer password is available to the technician and kept by the Mrs. Barnett, the Headteacher.
Staff and children are reminded of the importance of keeping passwords secure in the staffroom and during appropriate staff meetings.
If there is a breach of password security, the DSL is informed so that the passwords are changed as soon as possible via contacting the technician.
Passwords include numbers and symbols to ensure that they are secure and this is taught in the online safety education of children and staff.

Software/hardware

We ensure that we have legal ownership of all software (including apps on tablet devices) by following and purchasing from the correct places.
Where appropriate, licenses for all software are kept.
The technician installs and monitors any software installed on the laptops and computers. Mr. Wylde and the technician are responsible for iPad apps.

Managing the network and technical support

Technical security features, such as anti-virus software, are kept up-to-date and managed by technicians. Firewalls are switched on at all times.
Wireless devices are accessible only through a secure password.
Our iPads have restrictions on them preventing the downloading and deleting of apps and making 'in app' purchases.
Computers are monitored by our technician, who updates all computers/laptops when needed. They can be granted remote access if anything needs to be done immediately.
Staff are made aware of the safe and secure use of systems through rules taught during computing lessons.
Children are reminded to login and out of school systems correctly during every lesson.
Our technician is responsible for managing the security of our school network along with the support and vigilance of our staff. The safety and security of our school network is constantly monitored and adapted as it is needed.
Staff and children are not permitted to download executable files or install software and must seek the advice of the technician.
Users are to report any issues to the technician via the Western link on their desktop.

Filtering and virus protection

The system in school is monitored and managed by our technician.
All staff laptops are set to regularly update and staff are aware of this and comply with requests from our technician.

The governing board ensures the school's network has appropriate filters and monitoring systems in place. The governing board ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding. The DSL and technicians undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. Technicians undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the DSL. Prior to making any changes to the filtering system, technicians and the DSL conduct a risk assessment. Any changes made to the system are recorded by technicians. Reports of inappropriate websites or materials are reported to Mr. Wylde via an automated system, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behavioural Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the Child Protection and Safeguarding Policy.

11. Dealing with incidents

Any incidents are recorded by Mrs. Barnett, the DSL and stored securely. Decisions as to the course of action are discussed with and relevant bodies and any appropriate action is taken.

Illegal offences

Any suspected illegal material or activity is brought to the immediate attention of the DSL who will refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF).

Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.

It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident.

Potential illegal content is reported to the Internet Watch Foundation (**http://www.iwf.org.uk**).They are licensed to investigate – schools are not!
Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred.

More details regarding these categories can be found on the IWF website
http://www.iwf.org.uk

Inappropriate use

It is more likely that our school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence. Some examples of inappropriate incidents are listed below with suggested sanctions.

Incident Procedure and Sanctions

Accidental access to inappropriate materials.

- Minimise the webpage/turn the monitor off
- Tell the adult in charge
- Enter the details in the Incident Log and report to filtering services if necessary
- Persistent 'accidental' offenders will need further disciplinary action
- Using other people's logins and passwords maliciously
- Inform DSL
- Additional awareness, raising of online safety issues and the AUP with individual child/class
- More serious or persistent offences will result in further disciplinary action in line with Behaviour Policy
- We consider parent/carer involvement
- Deliberate searching for inappropriate materials
- Bringing inappropriate electronic files from home
- Using chats and forums in an inappropriate way.

12. Acceptable Use Policy (AUP)

The Willows Acceptable Use Policy stresses the importance of online safety training and education, is intended to ensure that all users of technology within school are responsible and are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes and reflects the content of the school's wider online safety Policy.
There are AUPs for staff, children and parents/carers that are available for all to access through the diaries and training.

Our AUP outlines the ways in which users are protected when using technologies, including passwords, virus protection and filtering.
Advice is provided for users on how to report any failings in technical safeguards.
All staff and children read and sign to agree to abide by the Acceptable Use Policy.

13. Education and Training

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond. They should, for example, be able to communicate safely and respectfully online, be aware of the necessity to keep personal information private, be taught how to search effectively and be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights.
The three main areas of online safety risk (as mentioned by OFSTED, 2013) that our school is aware of and considers are:

Content:

Children are taught, where appropriate (this is usually done using outside agencies, e.g. Childline.):

- That not all content is appropriate or from a reliable source
- About exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- About hate sites and cyberbullying
- Content validation: how to check authenticity and accuracy of online content.

Contact:

Children are taught, where appropriate (This is usually done using outside agencies, e.g. Childline.):

- That contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies
- About cyberbullying in all forms
- Issues with identity theft and sharing passwords.

Conduct:

Children are made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others (This is usually done using outside agencies, e.g. Childline.):

- Privacy issues, including disclosure of personal information, digital footprint and online reputation
- Health and well-being - amount of time spent online (internet or gaming)

- Copyright (little care or consideration for intellectual property and ownership – such as music and film).

Online safety - Across the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- HRSE
- PSHE
- Computing

Online safety teaching is always appropriate to pupils' ages and developmental stages.
Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of images and personal information
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate.

The online risks pupils may face online are always considered when developing the curriculum.
The DSL is involved with the development of the school's online safety curriculum.
Pupils are consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.
The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.
The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.
Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Online safety – Raising staff awareness

Online safety is discussed as and when issues appear, but always at the start of the year, staff are reminded of the rules and risks involved.

Online safety training aims to support staff with issues which may affect their own personal safeguarding e.g. use of Social Network sites?

Staff know that they are expected to promote and model responsible use of ICT and digital resources.

Online safety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

Parents/carers are updated and supported through school newsletters, homework diaries, our website and any other publications that may be deemed appropriate.

Online safety websites are clearly on display around school.

We promote external online safety resources/online materials through the newsletter and website.

14. Monitoring and Review

Any issues that are raised or observed are brought to the attention of the SLT and recorded and monitored. Decisions are then made as to whether action needs to be taken and often involves educating the children.

Regular questionnaires/discussions draw out the knowledge and understanding of each child.

The online safety scheme draws out understanding and assesses the needs and learning of the children.

This policy is reviewed at least annually and as necessary such as national changes or the purchase of new devices.