# The Willows Catholic Primary School

Online Safety Policy

Updated: Summer 2017

# Contents

1. Introduction
2. Our Vision for online safety
3. Our online safety Champion
4. Security and Data Management
5. Use of Mobile Devices
6. Use of Digital Media
7. Communication Technologies
8. Infrastructure and Technology
9. Dealing with incidents
10. Acceptable Use Policy
11. Education and Training
12. Evaluating the impact of the Online Safety Policy

# 1. Introduction

At The Willows Primary, 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 ICT and, at The Willows, it is a priority across all areas of the school.

# 2. Our vision for online safety

With the great speed at which technology that accesses the internet is becoming easily available in the forms of mobile phones, tablets, games consoles and smart TVs, it is imperative that all children 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 at The Willows, 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 or in the media 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; the online safety Policy being available from our website; holding online safety meetings for parents/carers and including relevant information in our Acceptable Use Policy that is renewed annually.

The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using technology. In delivering the curriculum, teachers need to 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 need 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 a staff meeting or lesson, 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 sound knowledge instilled 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. Our online safety Champion

Mrs. Barnett, the Headteacher, has the role of online safety champion, with the support of 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. 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 online safety champion 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 online safety Champion 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 Knight.
- ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- 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.
- 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 Child Exploitation and Online Protection Centre (CEOP).
- providing or arranging online safety advice/training for staff, parents/carers and governors.
- ensuring the Headteacher, SLT, staff, children and governors are updated as necessary.
- liaising closely with the school's Designated Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas. (Who is this?)

# 4. 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.
The *Lancashire ICT Security Framework* (published 2005) is consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school.
In line with the requirements of the Data Protection Act (1998), 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 currently remotely accessible by staff.
- Not held in any 'cloud' storage.
- 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 information on display in the staffroom.

# 5. Use of mobile devices

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."*

## 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.
Phones may be used during breaktimes, out of the sight and hearing distance of children. Designated areas are the staffroom, the office (if it is available) or the side of the building outside.
Personal devices must not be taken into EYFS and there are clear notices on the doors leading into those areas.
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.

### 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.

Parents are reminded about when they can take photos and videos and that they should only be of their child at the relevant events. It is also explained that they should not be used to show other children on social media sites.

*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. Therefore, if a mobile phone is brought to school, 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.

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

# **Other mobile devices**

## Staff

Staff are allowed to bring in other mobile devices, for example tablets, 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.

## Parents

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

## School

School has 8 ipads available for staff and children to use for educational purposes. 7 of the ipads are set up in the same format. One of them has been designated to the Lions class and has no internet access.

The ipads have restrictions on them to prevent children and staff from accessing itunes, the apple store, changing settings, deleting and installing apps, sending email, using facebook and using facetime. Age restricitions for apps and content have also been set up.

Mr. Knight has the restriction passcode and monitors this.

Content is downloaded through the official ipad app store use the head's account.

The ipads are stored in a cupboard in Mr. Knight's room when not in use. A timetable is in the staffroom to book out and monitor their use.

# 6. 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 the school diaries and consent is sought when a new child arrives.
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.

### Taking Photographs / Video

All classes have a camera with still and video capabilities and the class teacher and TAs connected to that class may use the camera for educational/school purposes. Children may also use the camera for educational purposes where they have been given permission. iPads also have the ability to take photographs and video footage but these are not linked to any cloud or wireless system. There are also no email accounts on them. Staff and children may use them as part of their learning but must remove any video or images as soon as they have been used.
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 Mrs Barnett 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 the Kirkham Swimming Baths and changing areas. 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

The class camera is kept hidden away in a drawer or cupboard in the classroom when not in use.

Any photographs/video footage of children are stored on a password protected laptop/computer. If they are transferred to a memory stick they are stored in a password protected area.

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) should not be sent via email without being password protected. Should they need to be sent that way for any purpose, they should be password protected and discussed with Mrs. Barnett, the Headteacher, before they are sent.

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 passed on to the person making the DVD and the photographs/video footage are deleted from the class cameras. (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 front of the child's diary.

Names must not accompany any photographs or video footage.

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 insecure sites e.g. personal Social Networking 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 with Mr. Knight any issues, especially 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.

# 7. 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.
The following are examples of commonly used technologies used in The Willows Catholic Primary School:

## Email

### Staff

All staff have access to the Lancashire Grid for learning service and are advised to use this for any email communications for school purposes.
Only official email accounts are used to contact other staff and parents/carers, and staff ensure 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 must not enter into email or text communications with children.
Staff are made aware of the dangers of opening emails that are classified as spam and need to be educated in good online safety in this area.
Staff are reminded (see the Acceptable Use Policy) that email communications may be monitored at any time.
Staff should report any inappropriate emails/ SPAM (Junk Mail) to Mrs. Barnett as soon as possible.

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 (1988) 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, in particular, 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.
The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts.

## Social Networks

Our school has a Facebook page, but the only staff with access are Mrs. Barnett, Mr. Wylde and Mr. Knight. There are to be no photographs, video footage or names posted to our Facebook page.
Staff have been informed that they should not like or post anything to our school Facebook page, especially using their own personal Facebook account.
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 must not be shared with children and privacy settings must be 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 must 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 should 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.
- They must not communicate with children using any digital technology, especially where the content of the communication maybe 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, must not be added as 'friends' on any Social Network site.
- They must not post inappropriate comments about staff or children that could be construed as instances of cyberbullying.
- They must 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.

## Instant Messaging or VOIP

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.
We do not allow any form of messaging through our website or VLE.

Parents are contacted through the teachers2parents.co.uk website but we are currently moving to a new app. This allows both forms to be completed and is also a messaging system. It is requested that any emails, where appropriate, are mentioned to Mrs. Barnes in case any parents phone with any questions or concerns. It is advisable that the content is discussed with Mrs. Barnett before being sent.

## Virtual Learning Environment (VLE) / Learning Platform

We use the Lancashire website and currently only staff have accounts and can access, modify or post things. Mr. Wylde is in charge of the website and has overall responsibility for its management, content and appearance. Teaching staff and members of the office have passwords and are made aware of security through the Acceptable Use Policy.
We use Activelearn where children have their own account. They are taught about online safety through ICT lessons. They can access learning, but cannot post anything that other children can see and they cannot access any external websites.

## Websites and other online publications

Our school website effectively communicates online safety to parents/carers through links to the thinkuknow website and childline website. Also through displaying the online safety policy online, suggesting reading material, for example, the digital parenting website, and providing support through Parent evenings on online safety.
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.

# 8. Infrastructure and technology

Our school ensures that the infrastructure/network is as safe and secure as possible. We subscribe to the Lancashire Grid for Learning/CLEO Broadband Service where internet content filtering is provided by default.
*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.*

Sophos Anti-Virus software is included in our school's subscription, and this is installed on all computers and laptops and is configured to receive regular updates.
Further information can be found at **www.lancsngfl.ac.uk/online safety**.

## Children's access

Children are supervised by a member of staff at all times when using computers/laptops/ipads/other devices in school.
Each year group has a login to access any computer/laptop.
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 are nearby. They should also ensure that the password is not given to others, especially written down, particularly supply teachers. Staff should check reasons for use and login supply teachers if this is necessary.
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, Mrs. Barnes/Mrs. Barnett or Mr. Knight are informed so that the passwords are changed as soon as possible via phoning 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.

Staff should note the guidelines in the Lancashire ICT Security Framework for Schools, available at **www.lancsngfl.ac.uk/online safety** website.

## 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. Paul Knight is responsible for ipad apps.

### Managing the network and technical support

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. Mr Knight has the password key and any requests should go through him.
Computers are monitored each week by our technician, who updates all computers/laptops when needed. He has 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 ICT 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 without the advice of our technician, Tom, and permission from Mrs. Barnett, The Headteacher.
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.

## 9. Dealing with incidents

Any incidents are recorded by Mrs. Barnett and kept in her office. Decisions as to the course of action are discussed with SLT and any appropriate action is taken.

### Illegal offences

Any suspected illegal material or activity is brought to the immediate attention of the Headteacher 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 LGfL filtering services if necessary.
- Persistent 'accidental' offenders will need further disciplinary action.
- Using other people's logins and passwords maliciously.
- Inform SLT or designated online safety Champion.
- Enter the details in the Incident Log.
- 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.

Staff are responsible for dealing with online safety incidents and reporting them to either Mrs Barnett, SLT or Mr. Knight

# 10. 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 website and the office.
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.

# 11. 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

It is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' online safety.

We have an online safety scheme that is progressive and is taught on top of online safety being reinforced throughout every lesson. We also focus on online safety when it is the Safer Internet Day in February.

Children are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.

Children are reminded of safe Internet through discussions and the lists of rules in the suite

## 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.

Bespoke Parents online safety Awareness sessions or workshops are held.

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

# 12. Evaluating the impact of the online safety Policy

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.