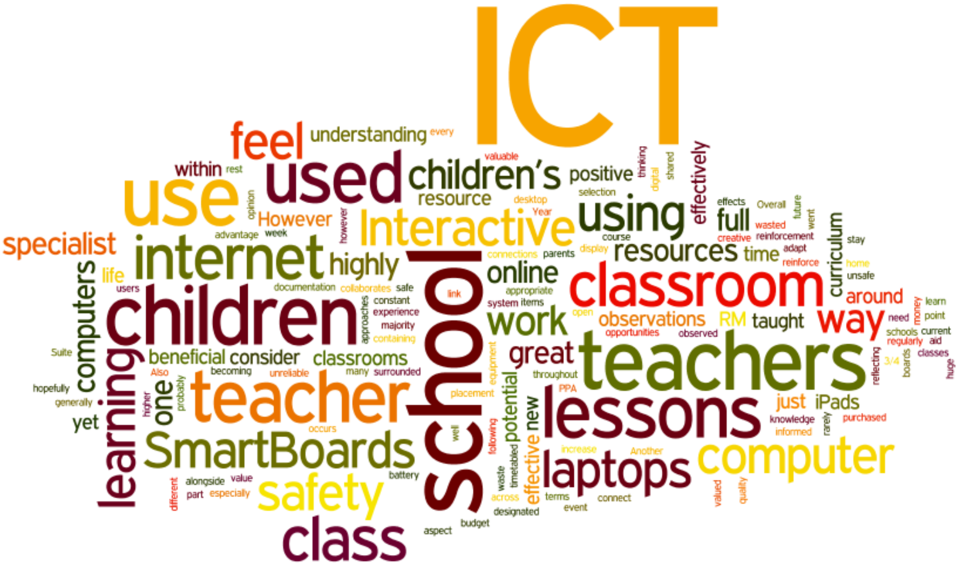
WEETON PRIMARY SCHOOL

Weeton
Primary School



Weeton Primary School

Online safety Policy 2023-2024

Weeton E-safety Policy 2023-2024

Contents

1. Introduction

At Weeton Primary, we see technology as a vital area of development in all subjects and endeavour to ensure that all staff and children have access to relevant, high quality technology. In many areas of school life, the use of technology is crucial and must be protected from disruption or loss of service. It is essential therefore 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, whether generic, cross curricular or for administrative purposes and, at Weeton, it is a priority across all areas of the school.

2. Our vision for online safety

With the incredible advances in the technologies that enable internet accesses, the internet is becoming easily available in the forms of mobile phones, tablets, games consoles and smart TVs, it is essential that all children at Weeton understand the benefits and dangers of using such devices. As the use of technology is an integral part of the teaching and learning at Weeton, we view the teaching of online safety as a key 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 also facilitate the teaching of this area in Upper KS2 through external specialists, such as WIRED, where available.

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; providing opportunities for an online safety meeting for parents and carers and including relevant information in our ‘Acceptable Use Policy’ that is reviewed regularly.

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 email. 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 a privilege for pupils who show a responsible and mature approach towards its use.

We ensure that children and staff at Weeton are protected in their use of technology through encouraging and modelling appropriate use, being supervised and having appropriate restrictions and filters in place.

Knowledge of what to do when problems occur is also a high priority for our school and this is delivered through staff meetings and sound knowledge instilled in children during lessons. This is crucial as children and adults need to also be aware of how they can deal with inappropriate content and contact when they are not in a school setting.

Computing and all it involves, such as e-mail, the internet and mobile devices are a vital part of our daily life in school and we therefore strive to give pupils and staff the opportunities to:

- access world-wide quality educational resources;
- participate in new initiatives;
- 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 Guru

Mr. Goth, the Headteacher, has the role of online safety Guru, with the support of Mrs. Hunt, and any problems, worries or concerns must be reported to him as soon as possible. If Mr. Goth is not available, the next person to report to is Mrs. Hunt. It should be noted that sharing/viewing illegal information/images with others is a criminal offence; however, it may be necessary to inform Mr. Goth in his role of online safety Guru to enable him to take further action if necessary and this may involve contacting the police.

The role of the online safety Guru 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 Mrs. Hunt

• 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/Backup DSP to ensure a co-ordinated approach across relevant safeguarding areas

4.Remote Learning

In the event of staff or children having to undertake remote learning as a result of Covid-19 related incidents, then work may be set for pupils using password protected online platforms; Purple Mash, TTRockstars, EspressoCoding, and Class Dojo. We also have a secure YouTube channel set up for staff to use where videos and tutorials may be uploaded.

Additional communication may also take place between staff and pupils via secure Edmodo class pages, which have been set up with parental permission and security measures. Any communication between parents/carers and staff will either be made via parentmail or directly from secure staff email accounts. For further information on remote learning, refer to our Remote Learning Plan which meets the expectations as set out in the DfE guidance 'Remote Education Support'.

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.

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

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 Mr. Goth (the Headteacher) in certain circumstances, for example, during pregnancy, illness or possible medical or family emergencies. Phones may be used during break times, out of the sight and hearing distance of children. Designated areas are the staffroom, the various offices (if available), Meeting Room, classrooms (if empty) or the side of the building outside.

Staff must seek permission from the Headteacher 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, including the playgrounds for drop off and collection.
Activities outside the normal school day (Sports day, class assemblies, shows, ECA events, Weeton Warriors) are all covered by the school Acceptable Use Policy.
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 without staff supervision.

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 class teacher as soon as the child arrives at school and is collected from the class teacher 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 Mr. Goth (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 without prior permission** and they must only be used to take photographs or video footage of children (tor Twitter etc) with prior permission from the Headteacher. Once uploaded, they must be deleted from the device. All images on devices can be checked by the HT or DHT at anytime.

Parents

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

School

School has 16 iPads per class for the children to use for educational purposes and one available for each teacher member of staff for educational and teaching purposes. Each class has their own iPads set up according for the classes needs and all iPads in a class are identical and set up in the same format.

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 restrictions for apps and content have also been set up. It is not possible for staff or pupils to edit this in any way.

The school technician controls and monitors the Apple content manager. Content is downloaded through the official BTLS store as recommend by Lancashire County Council.

Class iPads are stored in an iPad trolley and locked away each end of day or when not in use.

6. Use of digital media

(cameras and other 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. This is also sought for the use of Tapestry in Reception in order to create online Learning Journeys.

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 to them. Staff and children may use them as part of their learning, if appropriate, but must remove any video or images as soon as they have been used.

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 Mr. Goth as soon as possible so that he 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 Poulton 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 locked away in a 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 only 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 Mr. Goth and any other appropriate adults/parents/carers and permission from Mr. Goth should be sought. For example, dance festivals.

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 Mr. Goth, the Headteacher, before they are sent.

Staff do not store any images or video on their personal devices. In the summer term, any photographs or 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 with the child's admissions form in the main office. **A note is also put on SIMS for any child who does not have parental permission for images to be used.**

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 safeguarding training, staff meetings and online safety and blogging training, staff are reminded that:

- Children's names 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.

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 Weeton Primary School:

Email, Twitter, our password protected server network system.

Staff

All staff have access to the Outlook email 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 Mr. Goth, 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 Mr. Goth 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. They should report them to Mr. Goth or Mrs. Hunt, who will contact the appropriate E-safety team.

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 and turn off monitor.

Staff must report anything inappropriate/unexpected to Mr. Goth.

The Outlook filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts.

Social Networks

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, Instagram, TikTok, 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 Mr. Goth, 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.

Messages are now texted to parents. Staff involved 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 Mr. Goth or Mrs. Hunt 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.
- 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.

Any content posted online should not:

1. **bring the school into disrepute.**
2. **lead to valid parental complaints.**
3. **be deemed as derogatory towards the school and/or its employees.**
4. **be deemed as derogatory towards pupils and/or parents and carers.**
5. **bring into question their appropriateness to work with children and young people.**

Instant Messaging

These are all blocked through restrictions on the iPad and by the Netsweeper 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 are not to use school iPads for any personal communications. We allow messaging through our blogsite; however, replies are approved by teachers before they are visible.

Parents are contacted through Parentmail or directly by email. They also have access to the ParentMail app. This app allows parents and carers to pay online for school charges, such as dinner money and school trips.

Websites and other online publications

Our school website and Twitter page effectively communicates online safety to parents/carers through links to a wide range of informative and supportive websites. By displaying this online safety policy online, suggesting online safety web materials for example, the digital parenting website, and by providing support regarding online safety as and when required, Weeton Primary works hard to ensure parents/carers are not left worrying about the myriad of online safety issues out there alone, without support.

Only relevant staff have the ability to update information on the school website and Twitter account and training and discussions take place to ensure guidance is adhered to.

Overall responsibility for the website belongs to Mr. Goth, but responsibility for appropriate areas is delegated to relevant teaching staff.

Issues such as Copyright is strictly observed and discussed with children as part of their own online safety education.

Full names and personal details are not used on the website. Photographs are not named.

Any downloadable material is in the process of being 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

Weeton Primary ensures that its infrastructure and network is as safe and secure as possible. We subscribe to the **Netsweeper** 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. (Strategies are in place to deal with such situations.)

Sophos Anti-Virus software is included in our school's subscription is installed on all computers and laptops and is configured to receive regular updates.

Further information can be found at http://www.lancsngfl.ac.uk/onlinesafety/

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/pupil has a login to access any computer/laptop.

Computers/laptops are set up with the same format to ensure consistency for all.

iPads are set up with the same format per year group to ensure consistency for all.

Children cannot access any areas deemed not appropriate for example, administrator tools, due to password controls.

Adult access

Staff can access areas as are appropriate for their use and have access to only appropriate passwords. They are required to keep these confidential and to pass on to our IT technician immediately if they feel this has been breached.

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. In the case of supply staff, Mr. Goth or Mrs. Hunt could login into a generic login. For the register and SIMs reasons, **the class TA is trained** to access the register when needed. The administrator's password/installer password is available to the technician and kept by the Mr. Goth, the Headteacher.

Staff and children are reminded of the importance of keeping passwords secure at all times.

If there is a breach of password security, Mr. Goth or Mrs. Hunt are informed so that the passwords are changed as soon as possible by contacting our technician. In the case of a member of staff's login, **this needs to be regarded as urgent.**

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 legitimate authorised stockists.
- Where appropriate, licenses for all software are kept.
- The Technician installs and monitors any software installed on the laptops and computers. The technician is responsible for iPad app installation and deletion.

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. Any requests for apps go to Mr. Goth.

Computers are monitored fortnightly by our technician, who updates all computers/laptops when needed. He has remote access if anything needs to be done immediately. A form is available in the staffroom for reporting any non-urgent IT issues.

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. They are not allowed to turn on or off machines without permission or to shut down machines by simply pressing in the buttons as this could result in the loss of both other pupils and members of staff work.

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 needed.

Staff and children are not permitted to download executable files or install software without the advice of our technician and permission from Mr. Goth, the Headteacher.

Users are to report any issues to the technician via the form in the staffroom. Urgent issues can be emailed to LCC by the School Office or Mr Goth.

Filtering and virus protection

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

9. Dealing with incidents

Any incidents are recorded by Mr. Goth and kept confidentially. 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. 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.

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 E-safety Guru.
- 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.
- Once discovered inform SLT or designated E-safety Guru.
- 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.

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

10. Acceptable Use Policy (AUP)

Weeton 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. Effective Education and training - Safeguarding can be seen when:

In current times, 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.

Year on year there are new risks related to changes in society both on and offline. Staff have annual training and further updates, if required, to keep up with current trends and risks, so that they are always aware of tell-tales signs of abuse. NEW **Ofsted EIF** (Education Inspection Framework) **September 2019** tackles some more current trends…

- It is vital that **children and learners are protected and know how to get support if they experience bullying, homophobic behaviour, racism, sexism and other forms of discrimination.** Any discriminatory behaviours are challenged and help and support are given to children about how to treat others with respect.
- **Adults** understand the risks associated with using technology, including social media, **of bullying, grooming, exploiting, radicalising or abusing children or learners.**
- In cases of peer-on-peer abuse, **staff should consider what support might be needed for the perpetrators as well as the victims.**

'Adults understand that children's poor behaviour may be a sign that they are suffering harm or that they have been traumatised by abuse'

Taken from [Safeguarding In Schools]

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.

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 each class**.

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 eg. Many Facebook users are now removing surnames from profiles.

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

Online safety – Raising parent's/carer's 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, our website, blogsite and any other publications that may be deemed appropriate are disseminated.

Online safety guidance and websites are clearly on display on the **ICT Wall**.

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

For more advice click here: THINKUKNOW? CEOP YouTube channel Childnet guidance

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 further in a particular E-safety aspect or misconception.

Confidential questionnaires/discussions in ICT lessons reveal the knowledge and understanding of the children and also helps us to explore the needs and support required within the different classes and age groups.

E-safety Policy Information and Review

Academic Year	Designated Lead Person	Nominated Governor	Chair of Governors
2019-2020	Mrs S. Tuson	Pending	Cllr. C Little
2021-2022	Mrs N Hunt	Mr A Young	Cllr C.Little
2022 - 2023	Mr A Goth	Mr A Young	Cllr. C Little
2023 - 2024	Mr A Goth	Mr A Young	Cllr. C Little

E-safety Policy Review Dates

Review Date	Changes Made	By Whom
July 2021	Policy review and update	N. Hunt
Sept 2022	Policy review and update	A Goth
Sept 2023	Policy review and update	A Goth

E-safety Policy Approval by Governing Body

Academic Year	Date of Approval	Chair of Governors
2019-2020	Ov 2019	Cllr. C Little
2021-2022	Nov 2021	Cllr C Little
2022 - 2023	11 Nov 2022	Cllr C Little
2023 - 2024	14 Sept 2023	Cllr. C Little