Online Safety Policy

(including Acceptable Use Policy)

The Governing Body of West Street Community Primary School and Nursery adopted this policy on 01/09/21. The policy was last reviewed on 01/09/24 and will continue to be reviewed on an annual basis.

Our online safety vision statement;
To equip children with the skills and knowledge they need to use technology safely and responsibly at school, at home and beyond.

Online encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing such as online 'blogs' and online forums including Twitter and Facebook. Access to these technologies highlights the need to educate staff and pupils about the benefits and risks of using technology as well as providing safeguards and awareness for users to enable them to manage their online experience.

The school's Online Safety Policy operates in conjunction with other policies including those for Child Protection & Safeguarding, Behaviour, Anti-Bullying and Curriculum.

The purpose of these measures is to protect users, the school and LCC making the use of online technologies a safer and more enjoyable experience.

Good Practice Regarding Online Safety

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies
- Sound implementation of Online Safety Policy in both administration and curriculum, including secure school network design and use
- Safe and secure broadband from the Cleo Network including the effective management of Lightspeed Filtering Web filtering
- National Education Network standards and specifications

Further Information
For details of Online Safety in Lancashire schools;
School's ICT Centre 01257 516100
info@ict.lancsngfl.ac.uk
For cyber-bullying or digital safety concerns;

The Safer Internet Centre 0844 381 4772
helpline@saferinternet.org.uk
The following documents have been used for reference in the production of the Online Safety policy;

The Lancashire Online Safety Guidance Document and Framework Document

Both documents can be viewed and downloaded from;

http://www.lancsngfl.ac.uk/onlinesafety/index.php?category_id=13

Introduction

Writing and reviewing the Online Safety policy

The Online Safety Policy is part of the School Improvement Plan and relates to other policies including those for all curricular subjects, Behaviour, Anti-bullying, Child Protection & Safeguarding.

- The school's Online Safety Co-ordinator is Miss. Watson
- The school's Online Safety Champion is Mr. Smith
- Our Online Safety Policy has been written based on the Lancashire Online Safety Policy and government guidance. It has been agreed by the Leadership Team including EYFS leader, and approved by governors
- The Online Safety Policy and its implementation will be reviewed annually.
- The Online Safety Policy was revised by: Miss. Watson and Mr. Smith
- It was approved by the Governors:

The School's Online Safety Champion

The Online Safety Champion is the main point of contact for Online Safety related issues and incidents. The role of the Online Safety Champion includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable Use Policies
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored
- Ensuring 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 (APPENDIX 8 – Online Safety Incident Log)
- 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 Head, LT, staff, children and governors are updated as necessary
- Liaising closely with the school's Designated Senior Leader to ensure a coordinated approach across relevant safeguarding areas

Some of the above responsibilities may be delegated to appropriate members of staff.

Security and Data Management

ICT 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) should be 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 must be:

- 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.

All data in school must be kept secure and staff informed of what they can or cannot do with data through the Online Safety Policy and statements in the ICT Acceptable Use Policy

APPENDIX 3 –
ICT Acceptable Use Policy (AUP) – Staff and Governor Agreement
APPENDIX 4 –
ICT Acceptable Use Policy (AUP) – Supply Teachers and Visitors/Guests Agreement

Depending on your role in school you will have access to different network drives.
The headteacher has access to all areas.

Supply teachers only have access to the public drive so documents must be saved in their supply teachers folder. Always use the supply teacher login for supply teachers.

Data on the curricular and admin system is backed up locally daily by BT Connect remote backup. BT Connect monitors the back-up of data and deletes older back-ups when they are no longer required, all data is encrypted.

Staff are permitted to use pen drives and other similar devices to transfer none personal information such as lesson plans and resources for use in school and at home.

Staff are NOT permitted to use pen drives and other similar devices to transfer personal pupil information such as reports, tracking, children's names and pictures.

Assessment data, such as trackers, are stored on the Staff Shared drive on the school network, access to which is restricted by password to staff only. Staff are instructed not to store electronic copies of this data at home.

All user accounts are password protected. Staff have to change their password every 30 days for added security.

There is currently no remote access to school data from home other than

School does allow the use of 'cloud' storage facilities e.g. Dropbox / SkyDrive / Google docs and Moodle for external storage that is not confidential data.

We have three wireless networks in school.

The Use of Mobile Devices

School use of mobile devices, including laptops, tablets, mobile phones, cameras and games consoles is becoming more common. Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of online safety. Many of these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication.

Mobile phones

Mobile phones can present a variety of challenges if not used appropriately. Smart phones can upload pictures on to cloud storage so even if you delete pictures from a phone's memory, it is still stored on the cloud. They are valuable items that can be lost, stolen or damaged in the school environment and could also be considered as distracting or intrusive in a teaching or learning situation. However, staff and parents may equally have valid reasons why mobile phones should be readily available.

In order to balance the benefits of mobile phones alongside the possible issues they can create, the school has a number of guidelines in place:

- Staff are permitted to use mobile phones in school before the start of the school day, during break times, at lunch and after the school day has ended.
- Children are not permitted to have mobile phones in school
- In the event of a child bringing a mobile phone into school the phone is removed and stored in the office. Parents are contacted to remind them of the school rules regarding mobile phones
- Parents are asked not to use mobile phones inside the school premises or outside when a lesson is taking place. A notice is on display to remind visitors of this rule
- Staff are responsible for the security of their own belongings, including mobile phones. They can store them securely in the school office on request
- Staff are advised that it is good practice to store their mobile phones in 'silent' mode or off during lessons to reduce the risk of disturbance or inconvenience to others
- Images of children, video or audio must not be recorded on personal mobile phones

Safeguarding and Child Protection policy page 11 'USE OF MOBILE PHONES AND CAMERAS'

- The school office can always be contacted in the event of an emergency.
- Lunchtime staff leave their phones off or in designated areas
- **Warning!** Mobile phones have access to the Internet; this is NOT filtered and could lead to unsuitable content being viewed.

- Any suspicious use of mobile phones and / or cameras is report to the Headteacher or Deputy Headteacher

The Misuse of Mobile Phones

Mobile phones are one potential source of cyber bullying. The issue of cyber bullying is discussed with the children as part of the online safety/PSHE curriculum. The school reserves the right to confiscate a phone or device when there is good reason to believe that it is being used to contravene the school's behaviour policy. In the event of such action being required the headteacher or a member of the LT would be informed in order to manage the process and inform parents of the reasons for action.
Staff are asked to be vigilant in monitoring visitors for any covert use of mobile phones or cameras and to report any concerns to the headteacher.

Other mobile devices

The rules for mobile phone use in school apply to all other mobile devices.

- When permission to use such devices is granted it is expected that the relevant security settings, such as passwords and anti-viral protection, are in place and up to date
- The owners of the devices are responsible for ensuring that all the content held on them is legal and should understand that the school cannot be held liable e.g. for any damage or theft of personal devices
- Such devices can only be used on the school's network, e.g. to transfer data by Blue-Tooth or to access the Internet using Wi-Fi, after obtaining the express permission of the headteacher and should be checked first to ensure that they contain no viruses or mal-ware that may cause damage to the school's systems
- As with mobile phones, inappropriate use of such devices may lead to their confiscation

Use of digital media
(cameras and recording devices)

The use of cameras and sound recording devices offer substantial benefits to education but equally present schools with challenges particularly regarding publishing or sharing media on the Internet, e.g. on Social Network sites.
Photographs and videos of children and adults may be considered as personal data in terms of The Data Protection Act (1998).

Consent and Purpose

- Written consent is collected from parents for photographs of their children to be taken or used. Permission is given through a general written consent form issued to all families (Appendix 5 to 7)
- Staff are informed of any children whose parents or guardians have not given their consent for their photographs to be taken or their images used in digital form by the school. Every teacher is provided with a list relating to their class, a master list is kept in the office. It is the responsibility of staff to ensure that only images containing children whose parents or guardians have given permission are used by the school. Verbal consent is not considered acceptable. Images of staff or adults employed in the school will not be used without their written permission
- It is made very clear, when gaining consent, how photographs can / cannot be used (including the use of external photographers or involvement of 3rd parties)

- Written consent includes permission to store / use images once a child has left the school e.g. for brochures, displays etc. Parents should be informed of the timescale for which images will be retained
- Written permission forms will be issued to parents. In the event of any circumstances that may necessitate removal of permission, the list of children will be amended and reissued to all staff concerned
- Parents are informed of the purposes for which images may be taken and used e.g. displays, website, brochures, press and other external media
- Images that at times may be displayed in public areas e.g. the entrance hall, are subject to the same restrictions
- Parental permission is required for their child's images to be included in portfolios maintained by trainees and students not directly employed by the school
- Parental permission is required to use group images in individual children's profiles e.g. an image of a group activity in EYFS that is included in several children's profiles
- Images are not used of children or adults who have left the school unless their written permission has been obtained
- Written permission from parents is required when children's images are used by the press. Permission is required if the press wish to name individual children to accompany a photograph or if the media publish an image in their online publication which may offer facilities for the 'public' to add comments in relation to a story or image and can potentially invite negative as well as positive comments

Taking Photographs / Video

- Teachers and Teaching Assistants are authorised to take images related to the curriculum. Other adults taking photographs must be designated by the headteacher
- Photographs and videos are only taken using **school owned equipment**, including memory cards, digital tape and disks. The use of personal equipment to store images must be avoided
- When taking photographs and video the rights of an individual to refuse to be photographed are respected
- Photographs must never show children who are distressed, injured or in a context that could be embarrassing or misinterpreted
- Care is taken to ensure that individual children are not continually favoured when taking images
- The subject of any film or photograph must be appropriately dressed and not participating in activities that could be misinterpreted e.g. particular care may be needed with the angle of shots for children engaged in PE activities
- Certain locations are considered 'off limits' for taking photographs, e.g. toilets, cubicles, etc.
- Discretion must be applied with the use of close up shots as these may be considered intrusive. Shots should preferably include a background context and show children in group situations

Parents Taking Photographs / Videos

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 other purpose could constitute a potential breach of Data Protection legislation.

- Parents are informed that they should only take photographs of their own children and that they need permission to include any other children / adults.
- As it is virtually impossible for school to monitor parental pictures the school now publishes pictures on the school website after pictures are checked for permissions. If very high quality pictures are

uploaded they are put in a password protected part of the school website, the password is sent home in the newsletter but removed on the web version of the newsletter.
- Parents are reminded, in writing, that publishing images which include children other than their own or other adults on Social Network sites is not acceptable, unless specific permission has been obtained from the subjects and, in the case of children, their parents

Storage of Photographs / Video

- Photographs are securely stored and should not be removed from the school environment unless for a specific purpose and with the headteacher's consent. In this instance the data must be kept secure and must be erased after use. This could include storage of images on portable devices e.g. laptops or tablets
- Images should be stored on tablets for the minimal amount of time. Only images intended for a specific purpose should be stored. They must be stored securely and be deleted once they have been used
- Staff should not store images on personal equipment e.g. tablets, laptops or USB storage devices
- Staff should not store personal images on school equipment unless they have a clear purpose e.g. to support in the teaching of a lesson. Once used, the images should be deleted
- Access to photographs / videos stored on school's equipment is restricted to school staff. The server allows data to be stored so that it accessible either to all staff, teachers or pupils
- Individual members of staff are responsible for deleting photographs / video or disposing of printed copies (e.g. by shredding) once the purpose for the image has lapsed. The IT Technician has access to all areas of the network and can assist with the removal of data.
- Should a parent withdraw permission the class teacher is responsible for the removal and deletion of images and may be assisted by the Computing Subject Leader. Photographs sent electronically must be sent securely. This is done using staff accounts on the Lancashire e-mail system. Private email is not accessed in school using the school's equipment

Publication of Photographs / Videos

- Consent is needed from parents for publication of children's images, e.g. on a website
- Photographs should only be published online to secure sites
- When publishing photographs, care should be taken over the choice of images to ensure that individual children / adults cannot be identified or their image made available for downloading or misuse e.g. through the use of low definition images that will not magnify effectively e.g. using Image Resizer in Windows or the flash upload app on the school website
- Full names and / or other personal information should not accompany published images
- If very high quality pictures are uploaded they are put in a password protected part of the school website, the password is sent home in the newsletter but removed on the web version of the newsletter

When publishing images

- Children's images taken in school should not be displayed on insecure sites e.g. personal social networking sites. Parents and staff are informed in writing of this. If such images are reported their immediate removal will be requested
- Staff and children are made aware that full names and personal details will not be used on any digital media, particularly in association with photographs
- All staff should recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites. Staff should 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

The Media, 3rd Parties and Copyright

- Visiting third parties within school are supervised at all times whilst in the school and are expected to comply with the Data Protection requirements in terms of taking, storage and transfer of images
- The copyright for images taken by a 3rd party must be made clear beforehand and agreed by the school and parents before such images are used, eg in a local newspaper
- If uploading images to a 3rd party website, e.g. for printing or creating calendars, cards etc. staff are expected to read and be familiar with the terms and conditions of the website. (You could unknowingly be granting the site's host licence to modify copy or redistribute your images without further consent. The site may also be advertised for 'personal use' only – therefore using for business purposes would be a breach of the terms and conditions).

CCTV, Video Conferencing, VOIP and Webcams

- Parents should be informed if CCTV, video conferencing or webcams are being used in the school.
- Parents are required to give written permission for their child/children to participate in activities that include taking of video and photographs. Although children may not be appearing 'live' on the Internet through a video conferencing link, it is still 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
- Video conferencing (or similar) sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.
- The purpose for using CCTV /video conferencing or webcams should be made clear to those liable to be included in footage taken by these resources
- When used cameras should not overlook sensitive areas, e.g. changing rooms or toilets
- The headteacher would have overall access to any recordings made and would supervise their secure storage and deletion
- Consideration is required regarding copyright, privacy and Intellectual Property Rights (IPR) legislation
- Recordings are not repurposed in any other form or media other than the purpose originally agreed
- Image Consent forms can be found in Appendix 2

Communication technologies

School uses a variety of communication technologies, each of which carries various benefits and associated risks. All new technologies should be risk assessed against the potential benefits to learning and teaching before being employed throughout the school. Ideally this should be done before multiple devices are purchased. As new technologies are introduced, the Online Safety Policy will be updated and all users made aware of the changes. The policy is reviewed annually.

Email

- The Lancashire Office 365 service is the preferred school email system
- Staff should not access personal email accounts during school hours on school equipment unless prior permission is obtained from the headteacher and access is required for professional purposes.
- Currently children do not have e-mail accounts
- Only official email addresses should be used to contact staff or children
- Office 365 Learning filtering service is employed to reduce the amount of SPAM (Junk Mail) received on school email accounts
- All users should be aware of the risks of accessing content including SPAM, phishing, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail. Notices are displayed in staffroom of new SPAM outbreaks
- All users should be 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
- All users should also be aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy
- Staff are responsible for monitoring the content of children's email communications, both outgoing and incoming messages.
- Users must report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Children are taught how to respond in such situations by reporting immediately to the adult in charge at that time. Staff report to senior leaders within the school and can report to Lancashire directly.
- Users should be aware that they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act
- Our school includes a standard disclaimer at the bottom of all outgoing emails (see below).
  West Street school email disclaimer:
  ****
  This e-mail is confidential and privileged. If you are not the intended
  recipient do not disclose, copy or distribute information in this e-mail
  or take any action in reliance on its content.

  ****
  ****

All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

- We always tell an adult if we see anything we are uncomfortable with.

  APPENDIX 7 – Typical Classroom Online Safety Rules (EYFS KS1)

- We always tell a trusted adult if we find something that upsets us.

  APPENDIX 8 – Typical Classroom Online Safety Rules (KS2)

Social Networks

Social Network sites allow users to be part of a virtual community. They include sites such as Facebook, Twitter, Instagram, Bebo and Club Penguin. 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, it may be necessary to access and view other users' content, send messages and leave unmediated comments.
Many Social Network sites are blocked by default through filtering systems used in schools, but these settings can be changed at the discretion of the headteacher (See http://N.lancsngfl.ac.uk/lgfladvice/index.php for more details).
Where social networking sites are used, staff 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 need to be 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 be reviewed regularly to ensure information is not shared automatically with a wider audience than intended
- Staff 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 or lead to valid parental complaints. It should not be deemed as derogatory towards the school and/or its employees or towards pupils and/or parents and carers. It should not bring into question the appropriateness of staff to work with children and young people
- Adults must not communicate with children using any digital technology 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 should be discouraged
- Children must not be added as 'friends' on any Social Network site
- School's advice to parents in relation to their use of Social Networking Sites and how the school will respond to identified issues is: to refrain from posting inappropriate comments about staff or children that could be construed as instances of cyber bullying. Parents are also requested to refrain from posting 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

Instant Messaging systems, e.g. Text messaging, Skype, Facetime, are popular communication tools with both adults and children. They can provide an opportunity to communicate in 'real time' using text, sound and video. The Lancashire Grid for Learning filtering service 'blocks' some of these sites by default, but access permissions can be changed at the request of the headteacher
(See http://www.lancsngfl.ac.uk/lgfladvice/index.php for more details).

- Staff and children need to be aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts
- Staff do not use school equipment to communicate with personal contacts e.g. through 'Facetime' on an iPad
- Only secure messaging, forum or chat systems are used

- Any communication e.g. text messaging to contact parents, is to be kept secure and contact lists are stored securely in the school office.
- Virtual Learning Environment (VLE) / Learning Platform

Websites and other online publications

This may include for example: school websites, Social Network profiles, podcasts, videos, wikis and blogs. Information posted online is readily available for anyone to see and thus form an opinion about the school. From September 2012, the School Information (England) (Amendment) Regulations 2012 specified that certain up to date information must be made available on a school's website.

More details regarding these requirements can be found on the DfE website or at http://www.legislation.gov.uk/uksi/2012/1124/made

- The school website is used as one method to communicate Online Safety messages to parents/carers via links to Online Safety sites and access to the Online Safety policy
- Everybody in the school who is involved in editing and contributing to the website is made aware of the guidance for the use of digital media
- Everybody in the school should also be aware of the guidance regarding the inclusion of personal information on the website
- Editing online publications is restricted to staff who have the responsibility to ensure that the content is relevant and current
- Overall responsibility for what appears on the website lies with the headteacher in conjunction with the Computing Subject Leader
- Consideration is given to the use of any content subject to copyright/personal intellectual property restrictions
- Some content is occasionally hidden behind a password protected area e.g. links to governors information
- Downloadable materials in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re distributed without the school's consent
- YouTube is used for teaching if the page has already been checked beforehand
- Pupils are not allowed to use YouTube themselves
- Pupils are not allowed to use Facebook
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

Infrastructure and technology

School ensures that the infrastructure/network is as safe and secure as possible, West Street Primary School subscribes to the Lancashire Grid for Learning/CLEO Broadband Service and so internet content filtering is provided by default. The current filter is Lightspeed. 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 the school's subscription and is installed on computers in school by ED-IT then configured to receive regular updates.
Further information can be found at
http://www.lancsngfl.ac.uk/onlinesafety/

Children's access

- Children are always supervised when accessing school equipment and online materials (e.g.working with a trusted adult). Use of the computers at break and during lunchtimes is prohibited unless supervised by a member of staff
- Children access the school systems using class logins, individual logins and age appropriate passwords
- Children's access is restricted to certain areas of the network and computer

Adult access

- Access to school systems is restricted for all staff according to their areas of responsibility

Passwords

- All staff should be aware of the guidelines in the Lancashire ICT Security Framework for Schools. This is available at http://www.lancsngfl.ac.uk/onlinesafety/ website
- All adult users of the school network have a secure username and password. Passwords are changed every 30 days.
- The administrator password for the school network is only available to ED-IT
- Staff and children are reminded of the importance of keeping passwords secure
- Passwords can be changed at the individual's discretion by consultation with the Computing Subject Leader
- There is an agreed format for creating passwords for adults e.g. mixture of letters, numbers and symbols
- Passwords for classes follow name and number
- Passwords for children are made up by the children, they are taught to keep them secret

Software/hardware

- School has legal ownership of all software (including apps on tablet devices)
- School keeps an up to date record of appropriate licenses for all software. This is maintained by the ICT Technician
- An annual audit of equipment and software is made by the IT Technician
- The Computing Subject Leader, IT Technician and the headteacher control what software is installed on school systems

Managing the network and technical support

- Any servers, wireless systems and cabling are securely located and physical access is restricted
- All wireless devices have been security enabled
- All wireless devices are accessible only through a secure password
- Relevant access settings should be restricted on tablet devices e.g. downloading of apps and purchases

- HOLKER IT are responsible for managing the security of our school network. This is monitored by LCC
- School systems are kept up to date regularly in terms of security e.g. computers are regularly updated with critical software updates/patches and Sophos antivirus software is automatically updated
- Users (staff, children, guests) have clearly defined access rights to the school network e.g. They have a username and password and, where appropriate, permissions are assigned
- Staff and children are reminded to lock or log out of a school system when a computer/digital device is left unattended
- Users are not allowed to download executable files or install software. The IT Technician possess administrator rights and are responsible for assessing and installing new software
- Users can report any suspicion or evidence of a breach of security to the Computing Subject Leader, IT Technician or the headteacher
- School equipment, such as teachers' laptops or cameras, should not be used for personal/family use
- Any network monitoring takes place in accordance with the Data Protection Act (1998). Staff are told that the network may be monitored from time to time
- The Computing Subject Leader and IT Technician have been provided with a copy of this policy and are aware of the standards required to maintain Online Safety in the school

Filtering and virus protection

- IT system uses Lightspeed Filtering managed by BT Connect
- **Prevent Duty** - Lightspeed is compliant with the Government's current Prevent Duty guidance.
- (See https://education.btlancashire.co.uk/annual-services/education-bundle/internet-filtering.aspx for more details)
- Staff wishing to block or unblock websites may do so by making a request to the IT Technician. The IT Technician ensures that all equipment, such as school laptops, used at home are regularly updated with the most recent version of virus protection used in school
- Staff report any suspected or actual computer virus infection to the Computing Subject Leader or IT Technician

Dealing with incidents

An incident log (see Appendix 8) is completed to record and monitor offences. This is audited on a regular basis by the headteacher. Any suspected illegal material or activity must be brought to the immediate attention of the headteacher who must refer this to external authorities, e.g. Police, CEOPs or the 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.

Always report potential illegal content 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

See chart APPENDIX 11 – Responding to Online Safety Incident Escalation Procedures

Inappropriate use
It is more likely that 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.

Incident Procedure and Sanctions
Record on Incident Log – Appendix 10

In the event of accidental access to inappropriate materials;

- Minimise the webpage/turn the monitor off. Tell a trusted adult
- Inform the teacher who will enter the details in the Incident Log and report to the headteacher

If other people's logins and passwords are used maliciously, inappropriate materials are searched for deliberately, inappropriate electronic files are brought form home or chat forums are used in an inappropriate manner;

- Inform the designated Online Safety Champion
- Enter the details in the Incident Log
- Implement additional Online Safety training with the individual child or class
- Take appropriate action in relation to the disciplinary policy, e.g. contact parents.

Acceptable Use Policy (AUP)

The Acceptable Use Policy 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.

The AUP is provided for Staff, Children and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. The parental agreement is a partnership between parents/carers, children and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology will be kept in school and made available to all staff.

The AUP reflects the content of the school's wider Online Safety Policy and is regularly reviewed and updated. It is regularly communicated to all users and is understood by each individual user and relevant to their setting and role/ responsibilities. (Appendix 3 to 6)

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 need particular consideration are;

Content

Children need to be taught that not all content is appropriate or from a reliable source.
Examples of risk include;

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language) and substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact
Children need to be taught that contact may be made when using digital technologies and that appropriate conduct is necessary when engaging with these technologies. Examples of risk include:

- Grooming
- Cyberbullying in all forms
- Identify theft (including 'frape' – hacking Facebook profiles) and sharing passwords

Conduct

Children need to be aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves or others. Examples of risk include:

- Privacy issues, including disclosure of personal information, digital footprint and online reputation
- Health and well-being – amount of time spent online (internet or gaming)
- Sexting (sending and receiving of personally intimate images)
- 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' e-safety. We provide relevant, flexible and engaging Online Safety education to all children as part of their curriculum entitlement.

- Regular, planned Online Safety teaching takes place within a range of curriculum areas (including use of the Lancashire ICT Progression document)
- Online Safety education is progressive throughout the school. Staff are provided with a list of suitable sites, resources and activities for their year groups. This list is updated annually
- Teachers consider how Online Safety education can be differentiated for children with special educational needs
- We take part in the annual 'Safer Internet Day' activities that focus on Online Safety during the National Online Safety Awareness Week

- During lessons where the internet is used children are made aware of the relevant legislation when using the Internet e.g. Data Protection Act (1998) and copyright implications
- As part of the Online Safety training children are made aware of the impact of cyberbullying and how to seek help if they are affected by these issues, e.g. talking to a trusted adult in school or parent/carer
- Children are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions
- As part of their Online Safety training and PSHE children develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school
- Children are reminded of safe Internet use through corridor and classroom displays and the Online Safety rules that are displayed throughout school in all classrooms (Appendix 7 & 8).

Online Safety– Raising staff awareness

- Online Safety is regularly discussed during staff meetings and training
- Courses are available from Lancashire to train staff with overall responsibility for e-safety e.g. the Computing Subject Leader and Online Safety champion
- Online Safety training can be provided in school or by external agencies such as Lancashire Advisory Service and the police. (CEOP)

https://kcso.nspcc.org.uk/Login.aspx?ReturnUrl=%2flmshomepage.aspx

- Online Safety training and discussions ensure staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites
- All staff are expected to promote and model responsible use of ICT and digital resources
- Online Safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's Online Safety Policy and Acceptable Use Policy.
- The Online Safety Policy, Acceptable Use Policy, curriculum resources and general Online Safety issues are discussed regularly in staff/team meetings

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).

The school offers opportunities for parents/carers and the wider community to be informed about online safety, including the benefits and risks of using various technologies both at home and at school through:

- School newsletters, School Website and other publications
- Parents' Online Safety Awareness sessions or workshops
- Promotion of external Online Safety resources/online materials

Online Safety– Raising Governors' awareness

Governors, particularly those with specific responsibilities for online safety, Computing or child protection, are kept up to date through discussion at governor meetings, head teachers report, attendance at Local

Authority Training, CEOP or internal staff/parent meetings.

Evaluating the impact of the Online Safety Policy

There is a need to monitor and evaluate the impact of safeguarding procedures throughout the school. The headteacher and LT are responsible for the monitoring and evaluation of safeguarding (including online safety). Individual staff are responsible for the recording and reporting of incidents.

When monitoring takes place the school should consider:

- Is the Online Safety Policy having the desired effect?
- Are Online Safety incidents monitored, recorded and reviewed effectively?
- Is the introduction of new technologies risk assessed?
- Are these assessments included in the Online Safety Policy?
- Are incidents analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children and how can these patterns be addressed most effectively e.g. working with a specific group, class assemblies, reminders for parents?
- How does the monitoring and reporting of Online Safety incidents contribute to changes in policy and practice?
- How are staff, parents/carers, children and governors informed of changes to policy and practice?
- How often are the AUPs reviewed and do they include reference to current trends and new technologies?

Appendix List:

Appendix 1..... Change request for devolved filtering control – my LGfL Filtering Interface

Appendix 2 ..... Example of Image Consent Form

Appendix 3 ..... Example of ICT Acceptable Use Policy (AUP) – Staff and Governors

Appendix 4 ..... Example of ICT Acceptable Use Policy (AUP) – Supply Teachers, Visitors/Guests

Appendix 5 ..... Example of ICT Acceptable Use Policy (AUP) – Pupils

Appendix 6 ..... Example of ICT Acceptable Use Policy (AUP) – Parent's letter

APPENDIX 1 - Change Request for Devolved Filtering Control – my LGfL Filtering Interface

I would like to request devolved filtering control for my school through the my LGfL Filtering Interface. I understand that (with the exception of the mandatory 'Core Categories') this will allow the school to make local changes to the default filtering policies. Unless this is carefully managed, pupils and staff may have access to inappropriate content and materials and I accept that this would be the responsibility of the school.

I fully understand the implications this has relating to the wider Online Safety provision in school including the potential for misuse and can confirm that the school has the appropriate risk management policies and procedures in place to ensure this is managed accordingly.

Headteacher Name (print): ……...…

Headteacher LGfL email*: …….

Headteacher Signature: ……..……

Date: ……

School Name: ……

School District/Number: ……..……..…

* required for access to the LGfL filtering interface (e.g. head@exampleschool.lancs.sch.uk). Note: Colleagues using non-LGfL email addresses (e.g. hotmail, yahoo, .com etc) will be contacted directly with setup details. On completion by the Headteacher, please email the signed copy to 01257 516365. Changes will be actioned as soon as possible but, dependent on demand, may take up to 2 working days to take effect. 1 Important Note: It is inappropriate for unfiltered Internet access to be made available within school settings. Schools opting to take local control of their filtering policy should be aware of the wider implications of unblocking certain categories and sites and how they will maintain their statutory obligations under the safeguarding agenda (e.g. Social Networking – Cyberbullying, Media Sharing - Inappropriate content). We would therefore strongly advise that any delegation of filtering control is carefully considered and limited to only a small number of appropriate staff who are explicitly aware of the school's policies and procedures. It is advisable that the School Online Safety Policy should reflect how blocking access to inappropriate sites will be managed as part of the school's Online Safety escalation procedures.

APPENDIX 2 – Image Consent Form

Name of the child's parent/carer: _____

Name of child: _____

Year group: _____

We regularly take photographs/videos of children at our school. These may be used in printed publications, on our school website, or in school displays.

Occasionally, our school may be visited by the media who will take photographs/videos of an event or to celebrate a particular achievement. These may then appear in local or national newspapers, websites or on televised news programmes.

In order that we can protect your child's interests, and to comply with the Data Protection Act (1998), please read the Conditions of Use on the back of this form, then answer questions 1-4 below. Please sign, date and return the completed form (one for each child) to school as soon as possible.

(Please Circle)

1. May we use your child's photograph in printed school publications and for display purposes? **Yes / No**

2. May we use your child's image on our school website? **Yes / No**

3. May we record your child on video? **Yes / No**

4. May we allow your child to appear in the media as part of school's involvement in an event? **Yes / No**

I have read and understand the conditions of use attached to this form

Parent/Carer's signature:_____

Name (PRINT):_____

Date: _____

P.T.O

Conditions of Use

1. This form is valid for this academic year: 2023-2024

2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.

3. The school will not use the personal contact details or full names (which means first name and surname) of any pupil or adult in a photographic image, or video, on our website or in any of our printed publications.

4. If we use photographs of individual pupils, we will not use the full name of that pupil in any accompanying text or caption.

5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.

6. We will only use images of pupils who are suitably dressed.

7. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.

Notes On Use of Images by The Media - If you give permission for your child's image to be used by the media then you should be aware that:

1. The media will want to use any images/video that they take alongside the relevant story.

2. It is likely that they will wish to publish the child's name, age and the school's name in the caption for the picture (possible exceptions to this are large group or team photographs)

3. It is possible that the newspaper will re-publish the story on their website or distribute it more widely to other newspapers or media organisations.

APPENDIX 3 - ICT Acceptable Use Policy (AUP) – Staff, Student, Volunteer and Governor Agreement

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will be an active participant in Online Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.

3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.

4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.

5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

6. I will respect copyright and intellectual property rights.

7. I will ensure that all electronic communications with pupils and other adults are appropriate.

8. I will not use the school system(s) for personal use during working hours.

9. I will not install any hardware or software without the prior permission of Computing SL/HT

10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.

11. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

12. I will report any known misuses of technology, including the unacceptable behaviours of others.

13. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

14. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

15. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other user' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

16. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

17. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.

18. I will take responsibility for reading and upholding the standards laid out in the AUP.

19. I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

21. I understand it is my responsibility to ensure the safe use of technology by the children in my care as well as ensuring the devices/networks they access are looked after and will report any damage to the Computing Lead.

User Signature :

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

Signature ……..……..……

Date ……..……..……

Full Name ……..…… (PRINT)

Position/Role ……

APPENDIX 4 - ICT Acceptable Use Policy (AUP) Supply Teachers and Visitors/Guests Agreement

Mobile telephone: In our school the following statements outline what we consider to be acceptable and unacceptable use of Mobile telephones:

- Mobile telephones can be used in school by staff and visitors in designated areas only – the Staffroom and the PPA Room. They must not be used within the classroom
- Mobile telephones must only be used at non-teaching times, or break times, or in exceptional circumstances by specific prior arrangement with the Headteacher or Deputy Head
- Staff mobiles must be kept securely in own possession – school will not be responsible for the loss or damage to this personal equipment
- Notices will be displayed in staffroom as to the accepted use of mobile telephones.
- No images of staff or pupils in school will be taken on mobile telephones.
- Mobile telephones will not be used to support a lesson.

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

- All staff are aware that some mobile devices e.g. mobile phones, game consoles or net books can access unfiltered internet content
- All devices are virus checked before use on school systems
- Pupils are not allowed to bring mobile phones into school in any circumstance. If mobile phones are brought into school by a pupil they will be kept in the School Office until the end of the school day and then passed to parent/carer

For use by any adult working in the school for a short period of time:

1. I have read and understand the school's policy on the use of mobile phones and similar devices

2. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally

3. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory

4. I will respect copyright and intellectual property rights

5. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy, on school equipment and with written consent of the parent/carer or relevant adult

6. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image

7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems

8. I will not install any hardware or software onto any school system

9. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken

User Signature:

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

Signature ……..……..……

Date ……..……..……

Full Name & Position / Role

……..…… (PRINT)

APPENDIX 5 - Pupil Agreement / Online Safety Rules

These rules reflect the content of West Street Primary School's Online Safety Policy.

****NB Parents/carers MUST read and discuss all the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.**

- ✓ I will only use ICT in school for school purposes
- ✓ I will only use the Internet and/or online tools when a trusted adult is present
- ✓ I will only use my class e-mail address or my own school email address when emailing
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty
- ✓ I will not deliberately bring in inappropriate electronic materials from home
- ✓ I will not deliberately look for, or access inappropriate websites
- ✓ If I accidentally find anything inappropriate I will tell my teacher immediately
- ✓ I will only communicate online with people a trusted adult has approved
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- ✓ I will not give out my own, or others' details such as names, phone numbers or home addresses
- ✓ I will not tell other people my ICT passwords
- ✓ I will not arrange to meet anyone that I have met online
- ✓ I will only open/delete my own files
- ✓ I will not attempt to download or install anything on to the school network without permission
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe. I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my online safety
- ✓ I understand that failure to comply with this Acceptable Use Policy may result in being given consequences in line with the school's Behaviour Policy

We have discussed this Acceptable Use Policy with …….....
(print child's name) who agrees to follow the online safety rules and to support the safe use of ICT at West Street Primary School.

Parent /Carer Name (Print) ….……..……..…….

Parent /Carer (Signature) ….……..……..……...…….

Class …….. Date……..……

****When this AUP has been signed and returned then access to school ICT systems is allowed****

APPENDIX 6 – ICT Acceptable Use Policy (AUP) – Parent's Letter

WEST STREET PRIMARY SCHOOL

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and today's mobile technologies are an integral element of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all pupils to act safely and responsibly when using technology both within, and outside of, the school environment. This is particularly relevant when using Social Network Sites which are increasingly popular amongst both the adult population and young people. However, many sites do have age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of these age-restriction policies and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School Online Safety Policy and alongside the school's Behaviour Policy, outlines those principles we expect our pupils to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Along with addressing Online Safety as part of your child's learning, we will also be holding Online Safety Awareness Sessions during the school year, I would strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed.

In the meantime, if you would like to find out more about Online Safety for parents and carers, please visit the lancsngfl Online Safety website http://www.lancsngfl.ac.uk/Online Safety

Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguards the pupils in school.

When you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact Mr. Smith (Computing Subject Leader) or Miss. Watson.

Yours sincerely,

Miss. S. Watson (Headteacher)

APPENDIX 7 - Online Safety Rules (EYFS/KS1)

Our Golden Rules for Staying Safe with Computing
for EYFS & KS1

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

We always ask a trusted adult when we need help using the Internet.

We always tell a trusted adult when we find something that upsets us.

APPENDIX 8 - Online Safety Rules (KS2)

Our Golden Rules for Staying Safe with Computing for KS2

We always ask permission before using the internet.

We only use the internet when a trusted adult is around.

We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).

We always tell an adult when we see anything we are uncomfortable with.

We only communicate online with people a trusted adult has approved.

All our online communications are polite and friendly.

We never give out our own, or others' personal information or passwords and are very careful with the information that we share online.

We only use programmes and content which have been installed by the school.

APPENDIX 9 – Parental Online Safety Awareness Session

<Insert School's Letterhead>

This example letter has been used by schools when hosting a Parents Online Safety Awareness session run by a consultant from Lancashire Schools' ICT Team.

Dear Parent/Carer,

Having access to online information and the opportunities that the digital world can offer has many benefits and for some it plays an important part of our everyday lives. However, as technology moves on at such a pace, it is sometimes difficult to keep up with new trends and developments, particularly with regard to mobile/games technology and secure and safe accessibility to online material.

Our school has policies in place to ensure our children are learning in a safe and secure environment which includes being safe online. This session has been organised to help you to contribute to the process of helping your child to be aware of the potential risks associated with using the Internet and modern technologies.

Ofsted inspections increasingly view Parental Online Safety Awareness sessions as essential components of effective safeguarding provision and I would therefore appreciate your support in attending this event.

We will be hosting the above session on the Date/Time below and I would strongly encourage your attendance:

Date: Time:

The session will address the following areas with time for you to ask questions: What are our children doing online and are they safe? Do they know what to do if they come across something suspicious? Are they accessing age-appropriate content? How can I help my child stay safe online?

Yours sincerely,

<The Headteacher>

I / we will be attending the above Parental Online Safety Awareness Session

Name(s):_____

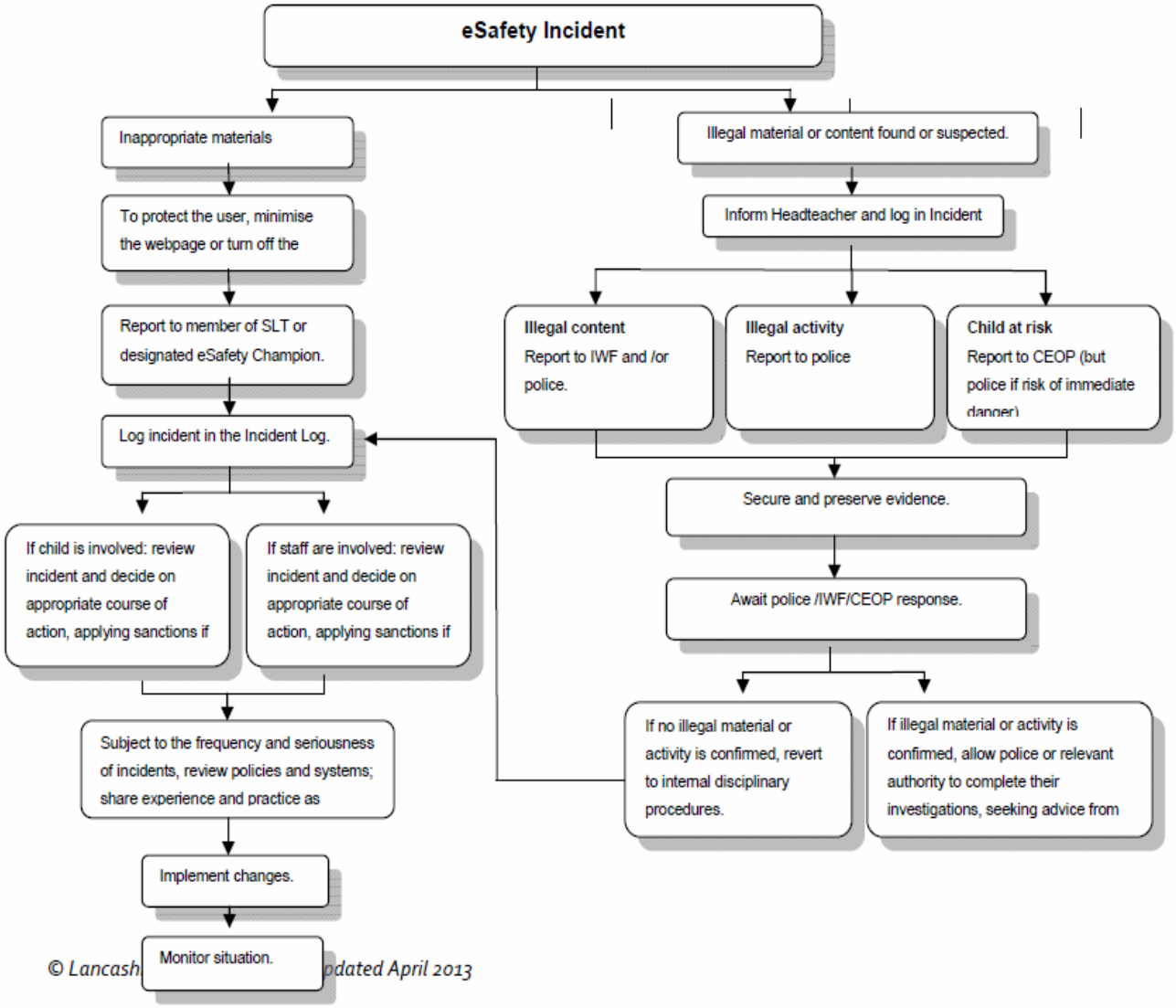
Parent / Carer of: _____ Year Group _____

APPENDIX 10 – Online Safety Incident Log

All Online Safety incidents must be recorded by the School Online Safety Champion or designated person. This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Governors. Any incidents involving cyberbullying should also be recorded on the Integrated Bullying and Racist Incident Record Form 2 available via the Lancashire Schools Portal.

Date / Time of Incident	Type of Incident	Name of pupil/s and staff involved	System details	Incident details	Resulting actions taken and by whom (signed)
01 Jan 2015 9.50 am	Accessing inappropriate website	A N Other (Pupil) A N Staff (Class Teacher)	Class 1 Computer	Pupil observed by Class Teacher deliberately attempting to access adult websites	Pupil referred to Headteacher and given warning in line with sanctions policy for 1st time infringement of AUP. Site reported to LGFL as inappropriate.

APPENDIX 12
Responding to eSafety Incident/ Escalation Procedures



Internet Watch Foundation
IWF Reporting Page:
www.iwf.org.uk/reporting.htm

Lancashire Constabulary
Neighbourhood Policing Team
www.lancashire.police.uk/contact-us
0845 1 25 35 45

Child Exploitation and Online Protection Centre (CEOP)
CEOP Reporting Page:
www.ceop.gov.uk/reportabuse/index.asp

LCC Schools' eSafety Lead
Lancashire Schools' ICT Centre
graham.lowe@ict.lancsngfl.ac.uk

Securing and Preserving Evidence – Guidance Notes

The system used to access the suspected illegal materials or activity should be secured as follows:

- Turn off the monitor (Do NOT turn off the system).
- Ensure the system is NOT used or accessed by any other persons (inc. technical staff).
- Make a note of the date / time of the incident along with relevant summary details.
- Contact your School's Neighbourhood Policing Team for further advice.