Online Safety Policy 2018

Background

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. It highlights the need to educate staff and pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

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

Introduction

Delph Side Primary School provides a diverse, balanced and relevant approach to the use of technology where children are encouraged to maximize the benefits and opportunities that technology has to offer. We ensure that the children in our care learn in an environment where security measures are balanced appropriately with the need to learn effectively and equip them with the skills and knowledge to use technology appropriately and responsibly. Our children are taught how to recognise risks associated with technology and how to deal with these risks both within and outside the school environment. We work with all members of our school community to educate them about the risks associated with technology and need for a school Online Safety policy

ICT in the 21st Century is an essential resource to support learning and teaching and a Delph Side as well as playing an important role in the everyday lives of children, young people and adults. Consequently we aim:-

"To equip children with the skills and knowledge they need to use technology safely and responsibly at the school, in the home and beyond."

We need to build in the use of these technologies in order to arm our young people with the skills to access lifelong learning and employment. New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.

- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

At Delph Side Primary School, we understand the responsibility to educate our pupils on Online Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

We must as a school demonstrate that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The Online Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

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.

Data Protection procedures have been reviewed in the Spring Term of 2018 to reflect on the changes in legislation with new General Data Protection Regulations (GDPR) that were implemented in May 2018 and a new Data Protection Policy is in place. Parents have been notified about the changes to data protection laws and updated privacy notices, which are available on the school website. (See Privacy Notice for Pupils in Letters Home on our school website). Staff have also been notified and received a privacy notice for the school workforce. Our consent forms have been updated and all parents have been asked to fill them in on Parent App, or by paper copy.

Online Safety Policy
June 2018

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 and Secure	Fairly and lawfully processed
Processed for limited purposes	Processed in accordance with the data subject's right
Adequate, relevant and not excessive	Kept no longer than is necessary and only transferred to others with adequate protection

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

- All teaching staff will log onto the school network with their own username and password and have access to the Teacher and Shared drives. All user accounts are password protected and staff have to change their password every 30 days for added security.
- Supply teachers only have access to the public drive so any work must be saved in the supply teachers folders. Always use the supply teacher login for supply teachers.
- Parent's workshops and other visiting groups have no access to any drives and are unable to save onto computers
- Data on the curriculum network is backed up daily onto external hard drives. There are two of these, while one is kept in a secure safe, the other is plugged into the main server for backups, the drives are swapped out each fortnight.
- Data on the admin network Is backed up remotely by Lancashire County Council and is also backed up daily onto an external drive.
- **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 must use encrypted memory drives** to transfer personal information such as reports, tracking, children's names and pictures. All teachers laptops are encrypted with True Crypt or Veracrypt.
- School does allow the use of 'cloud' storage facilities e.g. Dropbox / One Drive / Google docs for external storage that is none confidential data
- There are 2 wireless networks in school, all are secure:

The Use of Mobile Devices

School use of mobile devices, including laptops, tablets, mobile phones, cameras is becoming more commonplace. 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.

Online Safety Policy
June 2018

Mobile phones

Mobile phones can present a variety of challenges if not used appropriately. Smart phones can upload pictures onto cloud storage so even if you delete picture from phones memory, it's still stored on 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.
- Staff are responsible for the security of their own belongings, including mobile phones, and, on request, can store them securely in the school office. The school accepts no responsibility for the loss, theft or damage of such items.
- 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
- Mobile Phones will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff to use the school phone where contact with pupils or parents/carers is required.
- Staff should not use personal devices such as mobile phones or cameras to take audio, images or videos of pupils and will only use work-provided equipment for this purpose. The Headteacher gives permission for herself and members of the Senior Leadership Team to use their mobile phones when off site on residentials, educational visits and sporting events in order to be able to post updates for parents on Facebook. Photos are to be deleted off the device after the event and should ensure that they are not saved to any cloud storage

- Children are not permitted to have mobile phones in school. If absolutely necessary for a pupil to bring a mobile phone to school then pupil's mobile phones will be kept in the school office. Guidelines for mobile phones have been updated in line with Keeping Safe in Education 2018 which recognises that most children are using data on their phones, on the 3G or 4G network so we must ensure that children are not accessing the internet on personal devices when they're at school as this is **NOT** filtered and could lead to unsuitable content being viewed.

- If a child has to bring their mobile phone to school they must
  - Switch their mobile off at the bottom of the gate, when entering the school grounds, and put the mobile in their bag immediately
  - Hand their device to the school office(ensuring it is switched off)
  - The phone must be locked away for the duration of the day (the school does not accept responsibility for this device)

- Collect their phone at the end of the day and must ensure that no phone is switched on whilst on the school premises

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences
- Any suspicious use of mobile phones and / or cameras, report to Mrs Ormerod, Mr Fyne or Mrs Burton

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 Computing Curriculum as part of Online Safety and in our Jigsaw(PSHE curriculum). The school reserves the right to confiscate a phone or device if 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 head teacher or a member of the Senior Leadership Team would be informed and involved in the process and parents would be informed of the reasons for the action.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

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 head teacher.

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 access the Internet using Wi-Fi, after obtaining the express permission of the head teacher 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

Online Safety Policy
June 2018

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 and videos of their children to be taken or used. Parents consent to photos being published on the school website, Facebook and in the press.
- 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. Aiden, our ICT Technical Support Assistant, is responsible for compiling this list and updating it when new children join school.
- 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.
- 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 Facebook, 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.
- 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.

Taking and Publication 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**. The use of personal equipment to store images must be avoided.
- When taking photographs and videos 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.
- Photographs should only be published online to secure sites.
- Full names and / or other personal information should not accompany published images.
- 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.

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,
- Parents are reminded 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 Head teacher'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 also ensure that photos are deleted from the Recently Deleted album on the iPad.
- Staff should not store images on personal equipment e.g. tablets, laptops or USB storage devices. Any photos for class use must be on an encrypted memory stick.
- 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 ICT Leader and IT technician have 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 ICT 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.

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 read the terms and conditions of the web site. (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 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.
- 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.

Online Safety Policy
June 2018

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. 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.
- Office 365 Learning filtering service is employed to reduce the amount of SPAM (Junk Mail) received on school email accounts. Virtue Technologies filtering monitors and protects our internet access to the World Wide Web. We have desktop anti-virus protection from Sophos
- 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 put 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 should not access personal email accounts during school hours on school equipment unless prior permission is obtained from the Head teacher and access is required for professional purposes.
- Currently pupils do not have their own email accounts but this is to be looked into in the future with the best option to be considered for pupil use. School has a Google account(@delphside.com) and this would provide the facility to set up secure locked down emails for children where they would not be able to email outside @delphside.com using Google Apps for education.
- All pupil accounts would be Safe Email account and children would be taught how to use email as part of the curriculum eg pupils must immediately tell a teacher if they receive offensive e-mail, pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Users must report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Children will be 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.
- We will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law. We will reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- We know that spam, virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including

desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography and inappropriate language. ,

Social Networks

Social Network sites allow users to be part of a virtual community. They include sites such as Facebook, Twitter and Instagram. 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). 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 is 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.

Online Safety Policy
June 2018

School Facebook Page

At Delph Side we have a school Facebook book page and teaching and office staff have log in details

Rationale

Maintaining an online presence is vital for schools, not only in terms of keeping the school community up to date with what is happening in the school, but also in terms of attracting potential enrolment. Having a school website is an essential part of this, but web users must specifically visit the school website regularly to receive the information. By having a Facebook page, the schools is feeding school information, news and notices directly into the personal news feeds of parents and the wider school community.

Aims

The purpose of having a school Facebook page is

To continue to advance our school communication systems with information shared via Facebook, along with the existing methods of paper notes, text messages and the school website.	To publicise school events and increase awareness about school fund raising. To announce any updated information that appears on our website via Facebook
To highlight positive achievements in a forum where they can be shared by the school community	To make school announcements (eg school closure due to snow)
To use Facebook as a means of marketing the school to a wider audience	To engage the community that Delph Side serves and act as a key component of our online presence
To facilitate communication and networking opportunities between parents especially new or prospective parents	To maintain contact with past parents and past pupils

Terms of Use of Delph Side Facebook page

Users cannot advertise products or services on our school Facebook page	Users should not ask to become "friends" with staff as failure to respond may cause offence
Users should not post anything on the page that could be deemed as offensive – inappropriate or harmful comments/content will be removed immediately	Users cannot tag or post photographs. They are able to send these via message.
Users should not be giving negative feedback on Facebook, it is more appropriate to deal with the school directly on such matters	Staff members are able to post photos on posts to the school page, if school have consent from parents
Users will not mention individual staff members in a negative light on the school	Users should not add comments that can identify children

Facebook page	
Points to Note. Facebook lists a minimum age requirement of 13, and all parents are reminded that children under the age of 13 should not be on Facebook	

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

- 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
- Any communication, e.g text messaging to contact parents, is to be kept secure and contact lists are stored securely in the school office.
- Key Stage 2 children have access to an instant message feature on our school library system, The Reading Cloud. Children are able to add friends from in school and use a message feature to chat to their friends.
- Passwords are issued to children for the Reading Cloud and the children are taught to keep their details secret.
- Before accessing the Reading Cloud children are taught to use these communication tools in a responsible way in conjunction with the Online Safety curriculum. They are shown how to report any content that makes them feel uncomfortable by clicking the block button and informing Mr Fyne who is able to access the chat and monitor.

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.

- 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 and Facebook is made aware of the guidance for the use of digital media.
- 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 Senior Leadership Team.
- Consideration is given to the use of any content subject to copyright/personal intellectual property restrictions.

- 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
- Web site 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 Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Infrastructure and technology

School ensures that the infrastructure/network is as safe and secure as possible. Virtue Technologies provide the hardware that allows us to filter incoming traffic. The hardware itself is a Sophos UTM (more info:https://www.sophos.com/en-us/products/unified-threat-management.aspx). Virtue have full administration rights for the UTM and we have limited rights (things like the firewall are disabled and other configuration options) 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.

Security of Information Systems

The security of the school information systems will be reviewed regularly. Virus protection will be updated regularly. Files held on the school's network will be regularly checked. The ICT technician and technical support assistant will review system capacity regularly.

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Unapproved software will not be allowed.
- Files held on the school's network will be regularly checked.
- The ICT technician will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced. Staff have logins to the network and children gain access with generic year group log ins.

Children's access

- Children are always supervised when accessing school equipment and online materials .Use of the computers and iPads at break and during lunchtimes is prohibited unless in a supervised club.
- Children access to the school system is by a generic year group log in, eg y6. Children in Years 2 – 6 have a folder on the system to save their work in to.

- 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. Password are changed every 30 days.
- The administrator password for the school network are only available to the school technicians.
- 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 Aiden Roberts, technical support assistant.
- There is agreed format for creating passwords for adults e.g. mixture of letters, numbers and symbols.
- Passwords for classes follow y6, y5 etc

. **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 Aiden Roberts
- An annual audit of equipment and software is made.
- The ICT technicians, ICT Co-ordinator and the Headteacher control what software is installed on school system
- 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.
- Virtue Technologies are responsible for managing the security of our school network.
- 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 ICT Technicians 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 ICT Co-ordinator, ICT Technicians or the Headteacher.
- School equipment, such as teachers laptops and iPads 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 ICT Technician has been provided with a copy of this policy and is aware of the standards required to maintain Online Safety in the school.

Filtering and virus protection

- The school will work with Virtue Technologies, the school technician and the school technical support assistant to ensure that systems to protect pupils are reviewed and improved. The school technical support assistant has limited rights to blocking and unblocking sites.
- The school's broadband access will include filtering appropriate to the age and maturity of pupils. This is provided by Sophos
- The DFE published revised statutory guidance ' Keeping children safe in education'(May 2016). Schools are obligated to "*ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from school IT system*". See Appendix 1 from Sophos that illustrates that Sophos meets the national defined 'appropriate filtering standards'
- The School technician and technical support assistant 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 School technician and technical support assistant
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL must be reported to the technical support assistant who will take appropriate action.
- If staff or pupils discover unsuitable sites, the URL will be reported to the Computing co-ordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as CEOP

Dealing with incidents

Complaints of Internet misuse (including social networking concerns) will be dealt with by a senior member of staff.

- An incident log (see Appendix 6) is completed to record and monitor offences. This is also logged on CPOMS. This is audited on a regular basis by the Headteacher
- The Designated Child Protection Coordinator will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy include:
- A temporary or permanent ban on Internet use.
- Suspension of online learining site logins
- Additional disciplinary action may be added in line with the school's behaviour policies.
- Where applicable parents and other external agencies may be contacted.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County Online Safety Officer

All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community

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 12 – 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.

In the event of accidental access to inappropriate materials;

- Minimise the webpage/turn the monitor off. Tell a trusted adult.
- Inform or the Headteacher or ICT Subject Leaser who will enter the details in the Incident Log

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 Headteacher or ICT Subject Leader
- 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 Governors, 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 (see Appendix 2 to 4)

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 made 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 Policy
June 2018

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. Delph Side provides relevant, flexible and engaging Online Safety education to all children as part of their curriculum entitlement.

- Online Safety forms an integral part of our Computing curriculum, with half termly lessons from Active Bytes(our Online Safety planning) for each year group. This ensures that pupils are able to develop the skills to keep them safe online. It is revisited in the curriculum on a regular basis. Opportunities for learning about Online Safety are part of PSHE and reinforced whenever technology is used.
- Delph Side takes part in the annual Safer Internet Day each February, that focuses on Online Safety, and staff are provided with a list of suitable sites, resources and activities for their year groups. Each term there is an Online Safety assembly for Key Stage 1 and Key Stage 1 and we are responsive to new developments and will discuss issues with children, e.g Addictive Technology and new games such as Roblox and Fortnite.
- Delph Side provides opportunities for pupils to consider cyberbullying as part of Anti-Bullying week in the Autumn term.
- Teachers consider how Online Safety education can be differentiated for children with special educational needs.
- 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.
- 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 displays in the ICT and the Online Safety rules that are displayed in the ICT Suite and classrooms.

Online Safety– Raising staff awareness

- All staff will be given the School Online Safety Policy and Acceptable Use Policy and its application and importance explained.
- Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by the Head Teacher and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-safety Policy will be provided as required.
- Online Safety is also covered during our Safeguarding training
- Online Safety training can be provided in school or from external agencies such as Lancashire advisory service and the police. (CEOP)

- It is important that all staff feel confident to use new technologies in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies
- Staff must understand the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.
- Online Safety training/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.

ICT use is widespread and all staff including administrative, premises management, governors and teaching assistants are included in appropriate awareness raising and training. Induction of new staff includes a discussion of the school's Online Safety Policy, Acceptable Use Policy and Social Media Policy.

All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

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
- Regular promotion of the importance of Online Safety on the schools Facebook page
- Parents Online Safety Awareness sessions or workshops on Safer Internet Day
- Promotion of external Online Safety resources/online materials
- A partnership approach with parents will be encouraged

Online Safety– Raising Governors' awareness

Governors, particularly those with specific responsibilities for online safety, ICT 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. The Online Safety Policy is reviewed and approved by the governing body.

Date: June 2018

Online Safety Policy
June 2018

Written by: Mr Fyne

Appendices

Appendix 1 – Appropriate Filtering for Education Setting

Appropriate Filtering for Education settings

UK Safer Internet Centre
www.saferinternet.org.uk

June 2016

Provider Checklist Reponses

Schools in England (and Wales) are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*"[1]. Furthermore, the Department for Education published the revised statutory guidance 'Keeping Children Safe in Education'[2] in May 2016 (and active from 5th September 2016) for schools and colleges in England. Amongst the revisions, schools are obligated to "*ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.*"

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined 'appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Sophos
Address	The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP
Contact details	Spencer Parker, Product Line Manager, Web (spencer.parker@sophos.com 07929 055430)
Filtering System	Sophos XG UTM Appliance V16.0
Date of assessment	5th October 2016

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour	

[1] Revised Prevent Duty Guidance: for England and Wales, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

[2] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

for that question is AMBER.	

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
• Are IWF members		Yes
• and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		Yes
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Yes

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		Sophos has an "Intolerance and Hate" category where we categorize websites which fall into these categories and we would recommend the blocking of this category.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Sophos includes a controlled substances category in its URL data. We also have additional categories for "legal highs" and "Marijuana" and we would recommend the blocking of all three of these categories for schools.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Sophos includes these in our "Intolerance and Hate" category.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Sophos provides a number of categories to cover this. These are Anonymizers, Hacking, Phishing and Fraud, Spam URLs, and Spyware & Malware. In addition Sophos utilizes it anti-malware engines on all unencrypted content to detect malicious content. As an option, Sophos also offers a cloud-sandboxing solution called Sophos Sandstorm which takes any downloaded active content (e.g. executables or files with active content such as PDF or

the top unclassified websites are classified on an hourly basis. Sophos then provides this as a cloud service to our appliances so they always received the latest classifications for the URLs visited.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Sophos' category database is in use on over 300M devices worldwide which provides us a very large user community that report to us any misclassifications in our database. As we receive less than 50 of these requests per day (and most of which we do not reclassify as we believe them to be correct) we know the quality of our database is of the highest standard. We also provide a number of tools in the solution which help our customers. These include internal reclassification requests directly from the block page itself that go to the administrator of the solution to check if required and also the ability to create your own custom categories which override the current classifications from the URL database.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		Sophos XG UTM has the ability to generate policy rules based on group information. If the school includes objects in their directory that relate to age, then policies can be created that open up certain categories of websites once a certain year has been reached (e.g. sex education category). We also log all the groups of a user for reporting and these groups can be used to create reports for certain types of event. All alerts can also be sent out of the appliance via Syslog into almost any other alert monitoring system.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		The administration of the filtering solution is done by the school IT team (or one of their partners if this is out-sourced) and they have complete flexibility in the policy model to create a policy that can block categories, file types, URLs, IPs, and much more in an extremely user-friendly UI.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Sophos does not supply a recommended filtering policy for schools as it believes the school itself should create this. What we

		do provide is a rationale behind our web classification so accurate choices can be made by the IT admins around this. This information can be found at https://csc.cyberoam.com/cyberoamsupport/webpages/webcat/viewallcategorydescription.jsp
• Identification - the filtering system should have the ability to identify users		The Sophos XG UTM has a multitude of different ways of identifying users, both transparent (e.g. NTLM or SAML) and non-transparent (e.g. Captive portal)
• Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies		As the Sophos XG UTM can be deployed in a transparent mode, adding this to the guest Wi-Fi provided by schools is easy. Identifying the users is not so easy though, so you can choose to use a captive portal where the user would have to login first to be able to surf the web. If HTTPS decryption is deployed, the block page can show the certificate that needs to be added to the mobile device and instructions given on how to add this to the mobile device so the alerts are no longer seen. However, attempting to do HTTPS decryption on many mobile apps actually breaks them as they employ certificate pinning and you cannot decrypt their traffic. These would have to be manually added to the HTTPS decryption exceptions if the school wanted to allow the use of this app. Also this would not cover the device if it were using cellular (e.g 3G) data services, or if it leaves the school and uses another network (e.g. home broadband) for use.
• Multiple language support – the ability for the system to manage relevant languages		Yes, we support multiple block pages if we detect the language of the browser and custom block pages where you want to include multiple languages on the same page.
• Network level - filtering should be applied at 'network level' ie, not reliant on any		Sophos XG UTM can be deployed as a standalone web proxy or in

software on user devices		transparent bridge mode.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		Sophos XG UTM contains a number of inbuilt reports which can be used to see this information. In addition, the raw log files can be exported via Syslog to third party tools.
• Reports – the system offers clear historical information on the websites visited by your users		Sophos XG UTM contains a number of inbuilt reports which can be used to see this information. In addition, the raw log files can be exported via Syslog to third party tools

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum*".[3]

Please note below opportunities to support schools (and other settings) in this regard

Sophos has introduced Sophos Home (https://home.sophos.com) which provides home users free endpoint security software to block malware and enforce parental category controls for web traffic. This provides Enterprise-grade security free for home users that outperforms all other free anti-malware solutions and almost all paid-for solutions too.

In terms of education, Sophos in partnership with SWGFL have produced thousands of online educational booklets that are given to thousands of schools across the country to advise on online safety.

We also have student days at Sophos where we invite students into our head office in Abingdon to learn how Sophos deals with the latest online threats, and what students can do to better protect themselves.

It is also worth noting that many universities use Sophos products as part of their studies to learn about filtering and AV technologies

[3] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	STUART HILLINGHAM
Position	DIRECTOR
Date	16/01/16
Signature	

Appendix 2

Acceptable Use Agreement / Code of Conduct - Staff and Governors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff and Governors are aware of their professional responsibilities when using any form of ICT. All staff 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 Head Teacher

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
- I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils
- I will only use the approved, secure email system(s) for any school business.
- 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 users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not use or install any hardware (including USB sticks) or software without permission from the school technician.
- I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head teacher.

- I will respect copyright and intellectual property rights.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

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

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

- I will ensure that only children whose parents have given permission for them to use the Internet and ICT are enabled to do so at school.

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

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

- 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.

- I will take responsibility for reading and upholding the standards laid out in the AUP.I will support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies

.

- I 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.

- I will continue to abide by these rules, even if no longer a staff member or governor.

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

Signature …… Date ……

Full Name ……

Position / Role ……

Appendix 3

Acceptable Usage Policy – Students, Supply Teachers, Visitors, Guests

To be signed by any adult working in the school for a short period of time.

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
- I will not browse, download/upload or distribute any material that could be considered
  offensive, illegal or discriminatory.
- I will not use any external device to access the school's network e.g. pen drive, without the permission of the technician
- I will respect copyright and intellectual property rights.
- I will ensure that images of children 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.
- I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
- I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
- I will not install any hardware or software onto any school system.
- 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 ……..

Name……..……(PRINT)

Position/Role ……

Appendix 4

Acceptable Usage Policy KS1 Children –
Linked to 360 Safe AUP Guidelines

These rules have been written to make sure that you stay safe when using the computers. This includes cameras, laptops and webcams. By using the ICT in school, you have agreed to follow these rules. Your teacher will talk about these rules before you sign them and a copy will be sent home to you parents.
If you have any questions, please ask your teacher, Mr Upton or Fyne

The Golden Rule: Think before you click

- I will be careful when going on the internet
- I will only use the internet when a teacher is with me
- I will tell a teacher if I see something that upsets me
- I know people online might not be who they say they are
- I will be polite when talking to people or writing online
- I will think before I print or delete
- I will be careful when using or carrying equipment
- I will keep my password secret, but I can tell my family
- Remember to log off properly
- I will handle all computer equipment with care
- I won't tell anyone any personal details like my phone number or last name
- I won't log on the learning platform using someone else's username
- Never put water bottles on the table when using ICT

We have discussed this Acceptable Use Policy and
…….. [Print child's name] agrees to follow the eSafety rules and to support the safe use of ICT at *Delph Side Primary School*
Parent /Carer Name (Print)
……
Parent /Carer (Signature) ……
……..
Child (Signaure) ……

Class ……
Date……

Appendix 5

Acceptable Usage KS2 Children – Linked to 360Safe AUP Guidelines

These rules have been written to make sure that you stay safe and act responsibly when using the computers. When we talk about ICT, we are talking about computers, laptops, netbooks, and everything including cameras, web cams and tablets. These rules will have been discussed in class and a copy sent home to your parents.
If you have any questions, please ask your teacher or Mr Fyne.

Keeping Safe

- I will not use ICT in school without permission from my teacher
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will be careful when going on the internet. I will log off sites when I have finished
- I must keep my personal details and those of others private
- At all times, I will think before I click (especially when deleting or printing)
- I know that teachers can, and will, check the files and websites that I have used
- I will keep my usernames and passwords secure, but I understand that I can share them with appropriate people, such as my parents or teachers
- I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.

Communicating

- When communicating online (in blogs, emails, forums etc) I will think about the words that I use and will not use words that may offend other people. I know that I need to be polite and friendly online
- I am careful about what I send as messages as they can they can viewed by the E Safety co-ordinator and Headteacher
- When communicating online I will only use my first name and not share personal details such as my email address or phone number
- I understand that people online might not be who they say they are
- I will talk to an adult if an online friend want to meet me and never arrange to meet anyone without permission
- I will not log on the learning platform using another child's account
- I will **NOT** contact any member of staff via social networking site
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.

Research and Fun

- When using the internet, I will think about the websites that I am accessing
- I will not deliberately look for, or access inappropriate websites.
- I will use clear search words so that I find the right information
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site

Online Safety Policy
June 2018

Sharing

- I will not look at other people's files or documents without their permission
- I will not install any software or hardware (including memory sticks) or try to change computer setttings without permission from the teacher
- 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 not take or share pictures of anyone without their permission
- I know that anything I put up on the internet can be read by anyone

Problems

- If I find a website, image or message that is inappropriate, I will tell my teacher straight away
- I will take care when using the computers and transporting equipment around. I will tell a teacher if equipment is broken or not working
- I understand that if I am acting inappropriately then my parents may be informed and access to the learning platform may be suspended

- 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 E Safety.

- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

We have discussed this Acceptable Use Policy and
…….. [Print child's name] agrees to follow the eSafety rules and to support the safe use of ICT at *Delph Side Primary School*
Parent /Carer Name (Print)
……
Parent /Carer (Signature) ……
……..
Child (Signaure) ……

Class …… Date……

Appendix 6

Delph Side Primary School Online Safety Incident Log

Details of ALL Online Safety incidents to be recorded in the Incident Log. This incident log will be monitored termly by the Head teacher.

Online Safety Incident Log

Name of child:_____

Date:

Reported by:

Room and computer / device _____

Details of incident (incl evidence) Signed:_____

Actions and Reasons

Signed:(DSL)_____ Date:_____

Appendix 7

Advice for Parents and Children on Cyber-bullying

Key Safety Advice

The whole school community has a part to play in ensuring cyber safety. Understanding children and young people's online lives and activities can help adults respond to situations appropriately and effectively. Asking children and young people to show adults how technologies and services work is a useful strategy that can provide an important learning opportunity and context for discussing online safety.

For children and young people

1: Always respect others – be careful what you say online and what images you send.
2: Think before you send – whatever you send can be made public very quickly and could stay online forever.
3: Treat your password like your toothbrush – keep it to yourself. Only give your mobile number or personal website address to trusted friends.
4: Block the bully – learn how to block or report someone who is behaving badly.
5: Don't retaliate or reply!
6: Save the evidence – learn how to keep records of offending messages, pictures or online conversations.
7: Make sure you tell:
   - an adult you trust, or call a helpline like ChildLine on 0800 1111 in confidence;
   - the provider of the service; check the service provider's website to see where to report incidents;
   - your school – your teacher or the anti-bullying coordinator can help you.

Finally, don't just stand there – if you see cyberbullying going on, support the victim and report the bullying. How would you feel if no one stood up for you?

For parents and carers

1: Be aware, your child may as likely cyberbully as be a target of cyberbullying. Be alert to your child seeming upset after using the internet or their mobile phone. This might involve subtle comments or changes in relationships with friends. They might be unwilling to talk or be secretive about their online activities and mobile phone use.
2: Talk with your children and understand the ways in which they are using the internet and their mobile phone. See the seven key messages for children (on the left) to get you started.
3: Use the tools on the service and turn on in-built internet safety features.
4: Remind your child not to retaliate.
5: Keep the evidence of offending emails, text messages or online conversations.
6: Report cyberbullying:
   - Contact your child's school if it involves another pupil, so that they can take appropriate action.
   - Contact the service provider.
   - If the cyberbullying is serious and a potential criminal offence has been committed, you should consider contacting the police.

Appendix 8 – Roles and Responsibilites

Role	Responsibility
Governors	• Approve and review the effectiveness of the E-Safety Policy and acceptable use policies • E-Safety Governor works with the Headteacher to carry out regular monitoring of E-safety incident logs, filtering, changes to filtering and then reports to Governors
Headteacher and Senior Leaders	• Ensure that all staff receive suitable CPD to carry out their e-safety roles and sufficient resource is allocated. • Ensure that there is a system in place for monitoring e-safety • Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff • Inform the local authority about any serious e-safety issues including filtering • Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented.
E-Safety Leader	• Deal with day to day E-Safety issues • Lead role in establishing / reviewing e-safety policies / documents, • Ensure all staff are aware of the procedures outlined in policies • Provide and/or brokering training and advice for staff, • Attend updates and liaising with the LA e-safety staff and technical staff, • Deal with and log e-safety incidents including changes to filtering, • Report regularly to Senior Leadership Team
Teaching and Support Staff	• Participate in any training and awareness raising sessions • Have read, understood and signed the Staff Acceptable Use Agreement (AUP) • Act in accordance with the AUP and e-safety policy • Report any suspected misuse or problem to the E-Safety Co-ordinator • Monitor ICT activity in lessons, extra curricular and extended school activities
Students / Pupils	• Participate in e-safety activities, follow the acceptable use policy and report any suspected misuse • Understand that the E-Safety Policy covers actions out of school that are related to their membership of the school
Parents and carers	• Endorse (by signature) the Student / Pupil Acceptable Use Policy • Ensure that their child / children follow acceptable use rules at home • Discuss e-safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet • Access the school website in accordance with the relevant school Acceptable Use Policy. • Keep up to date with issues through school updates and attendance at events
Technical Support Provider	* Ensure the school's ICT infrastructure is secure in accordance with Becta guidelines and is not open to misuse or malicious attack • Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data • Inform the head teacher of issues relating to the filtering • Keep up to date with e-safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction. • Ensure monitoring software / systems are implemented and updated • Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and that reasonable attempts are made to prevent spyware and malware.
Community Users	Sign and follow the AUP before being provided with access to school systems.

Appendix 9

Notes on the legal framework

This section is designed to inform users of legal issues relevant to the use of communications. It is not professional advice.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the child to 18 years old;
The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and I The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.
N.B. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
More information about the 2003 Act can be found at ***www.teachernet.gov.uk***

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent : there is no need to prove any intent or purpose.

Data Protection Act 1998 / General Data Protection Regulations 2018

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:
gain access to computer files or software without permission (for example using someone else's password to access files); gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or impair the operation of a computer or program (for example caused by viruses or denial of service attacks). UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.
It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.
It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudophotographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.
Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

E-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Click Clever Click Safe Campaign: http://www.nidirect.gov.uk/click-clever-click-safe
Cybermentors: www.cybermentors.org.uk
Digizen: www.digizen.org.uk
EIS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk
Internet Watch Foundation (IWF): www.iwf.org.uk
Kidsmart: www.kidsmart.org.uk
Schools e–Safety Blog: www.kenttrustweb.org.uk?esafetyblog
Think U Know website: www.thinkuknow.co.uk
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Appendix 11 – Online Safety Letter for Parents

Delph Side Community Primary School

Eskdale, Tanhouse, Skelmersdale, Lancashire WN8 6ED
Tel: (01695) 721881
e-mail: head@delphside.lancs.sch.uk
web-site: www.delphside.lancs.sch.uk

Headteacher: Mrs Ormerod

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network Sites that incorporate 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 the site's privacy policy and / or terms and conditions 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 and Safeguarding Policies outlines those principles we expect our children 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. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Along with addressing Online Safety as part of your child's learning, we will also be holding Parental Online Safety Awareness Sessions during the school year and I would take this opportunity to 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 E Safety website http://www.lancsngfl.ac.uk/esafety

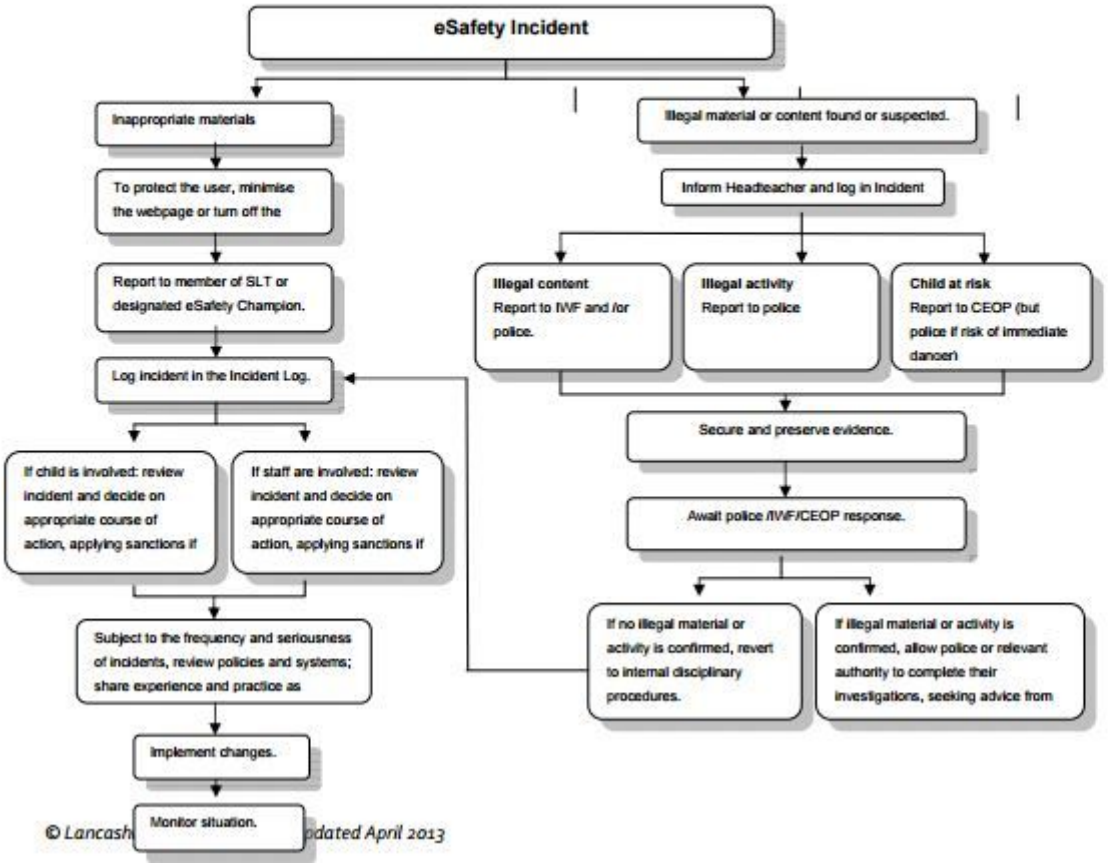
If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact *Mr Fyne or Mrs Ormerod*

Yours sincerely,

Mrs Ormerod

Appendix 12 - Responding to Online Safety Incident Escalation Procedures

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.

© Lancash *dated April 2013*

Online Safety Policy
June 2018