Online Safety Policy 2019

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.

This policy applies to all members of the Delph Side community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

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, Mobile Phone Policy, Password Policy and Data Protection Policy.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the *school*.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

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

Online Safety Policy
June 2019

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.

Education and training

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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 2 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 teaching 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 tezching 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.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use. Systems are in place for dealing with any unsuitable material that is found in internet searches (see reporting).
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Online Safety– Raising staff awareness

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.

- All staff will be given the School Online Safety Policy and Acceptable Use Policy and its application and importance explained.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy, Acceptable Use policy, Mobile Phone Policy and Social Media Policy.
- 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 Online Safety Policy will be provided through briefings during the year.
- An audit of the online safety training needs of all staff will be carried out regularly
- Online Safety is 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.
- The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organizations and provide guidance and training as and when required.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

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:

- Reference to relevant websites and app guides on our Online Safety page on our website
- Regular promotion of the importance of Online Safety on the schools Facebook page and on Seesaw
- Parents Online Safety Awareness sessions or workshops on Safer Internet Day
- Promotion of external Online Safety resources/online materials
- Parent Online Safety forums
- A partnership approach with parents will be encouraged

Online Safety– Raising Governors' awareness

- Governors are invited to our annual safeguarding training that includes online safety training.
- Our Online Safety governor has completed the NSPCC Online Safety training and other governors have an opportunity to complete annual online safety training from Safeguarding Essentials.
- The Online Safety governor is part of the Online Safety group
- Governors are kept up to date with issues of online safety through the Online Safety report to Governors
- The Online Safety Policy is reviewed and approved by the governing body.

Online Safety Policy
June 2019

Online Safety - The Wider Community

Delph Side will provide opportunities for local community groups / members of the community to gain from the academy's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents, on Facebook and Seesaw
- The Online Safety page on our website will provide online safety information for the wider community

Data Protecion

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. Jo Whitfield is the Data Protection Officer.

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 60 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, with passwords,** 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:

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

<u>The Use of Mobile Devices (including BYOD devices)</u>

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. (see Mobile Phone Policy). The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching

about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

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

- 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. Use of phones must be limited to non-contact time when no children are present.
- 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.
- Phones **MUST** be kept out of sight (eg. drawer, handbag) when staff are with children.(***Phones should not be in pockets***)
- Staff **MUST** ensure that mobile phones are 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, e.g acutely sick relative.
- 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. Consent forms to be completed and signed.

- The Headteacher is able to use her phone to take photos to post on Facebook for promotional purposes. Photos are to be deleted off the device after the event and should ensure that they are not saved to any cloud storage.

Pupils:

- 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. Children must complete a mobile phone consent form.
- 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.
    - Use of social media, text messages or the Internet is not permitted on school grounds.

- 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
- Pupils are not permitted to have mobile phones on educational visits or residentials.

Parents, Visitors and Volunteers:

- Adults either in school or accompanying children on school trips should not use their cameras or mobile phone cameras to take pictures of pupils unless it is at a public event such as Sports day or Summer fair and of their own children.
- Use of phones must be limited to non-contact time when no children are present.
- Personal cameras and mobile phone cameras should not be used to take pictures of children.
- If parents who accompany children on a school trip are asked by the teacher to take photos as a record of the educational visit, they will be issued with a school iPad.

- Parents will be allowed to take photographs at school events, eg Nativity performances, graduation, but will be reminded that they should only share photos of their child on Social Media, and not any other children.

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 Active Bytes, Online Safety, curriculum 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

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.

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 2019

The table below indicates which devices are allowed and defines their access to school systems.

	Allowed in school	Full Network Access	Internet Only	No Network Access
School Devices				
School laptops – Staff	/	/		
Ipads – Staff	/		/	/
Ipads - Children	/		/	/
Personal Devices				
Mobile phones(Staff) **** Must not be used around children* See Mobile Phone Policy***	/		/	/
Mobile phones (Pupils)	No #			/
Laptops/iPads (Staff)	/		/	/
Personal devices (visitors)	/			/

Unless signed consent and device is switched off and left in the office (see mobile phone policy)

<u>Use of digital media (cameras and recording devices)</u>

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

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, Seesaw 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. Aidan, 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 and on Seesaw.

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**. T
- 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. Consent forms to be completed and signed.
- The Headteacher is able to use her phone to take photos to post on Facebook for promotional purposes. Photos are to be deleted off the device after the event and should ensure that they are not saved to any cloud storage.
- 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 or bring the individuals or school into disrepute 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

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school / events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students* / *pupils* in the digital / video images.
- 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 2019

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. 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. ,

Use of Social Media

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimize the risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

All staff **need** to be aware of the following points:

- The content on Social Network sites may be unmediated and inappropriate for certain audiences.
- 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,
- 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.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to Delph Side Primary School.
- 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.

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- 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.

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

Online Safety Policy
June 2019

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 Facebook page	Users should not add comments that can identify children
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
- Class teachers use the Seesaw app as a communication tool with parents. This allows parents to individually message parents. Parents are aware that replies to messages may not be received out of work hours, and they will get replies the next day.

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 technical security

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Online Safety Policy
June 2019

School ensures that the infrastructure/network is as safe and secure as possible. We use Sophos UTM (more info:https://www.sophos.com/en-us/products/unified-threat-management.aspx). Our school technicians have full administration rights. 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. There will be regular reviews and audits of the safety and security of school / technical systems.

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 when children are in Key Stage 1 and in Year 3.
- Children in Year 4 – 6 have their own log in to the school network that should be used at all times. Children in Year 3 will be given their own log in during the summer term.
- 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 60 days.

- The administrator password for the school network are only available to the network managers.
- The "master / administrator" passwords for the school ICT systems, used by the Network Manager must also be available to the *Headteacher* / or other nominated senior leader and kept in a secure place (eg school safe)
- **All staff users will be provided with a username and password** by the ICT technician who will keep an up to date record of users and their usernames.
- the password should be a minimum of 7 characters long and must include three of – uppercase character, lowercase character, number and/or special characters
- must not include proper names or any other personal information about the user that might be known by others
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- **passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school**
- should be changed at least every 60 days
- should not be re-changed within 7 days of changing to a new password, nor re-use an existing password from within a cycle of 12 password changes by the same user.

.Software/hardware

- School has legal ownership of all software (including apps on tablet devices).
- Aiden Roberts is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- 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.
- Phil McCauley and Aiden Roberts 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 DNS Filter, the school technician and the school technical support assistant to ensure that systems to protect pupils are reviewed and improved.
- The schools has differentiated user level filtering.
- The school's broadband access will include filtering appropriate to the age and maturity of pupils. This is provided by Sophos and DNS Filter.
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored
- The DFE published statutory guidance ' Keeping children safe in education'(September 2018). 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 DNS Filter 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.
- 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
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach.

- If staff or pupils discover unsuitable sites, the URL must be reported to the technical support assistant who will take appropriate action. In school we use CPOMS but also have a paper based reporting tool.
- If staff or pupils discover unsuitable sites, the URL will be reported to Aiden Roberts who will then record the incident and escalate the concern as appropriate and add to the blacklisted websites.

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (see appendix 9) for responding to online safety incidents and report immediately to the police.

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). Further advice on how to deal with sexual images at work can be found at https://www.iwf.org.uk/resources/how-to-deal-child-sexual-abuse-images-at-work

Other Incidents

It is hoped that all members of the school will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action

- **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

- Incidents relating to Online Safety are logged on CPOMS. These are then dealt with by a Designated Safeguarding Lead, in association with the Online Safety leader. In addition there is also an Online Safety reporting log (available in the staffroom) that can be used.
- These are audited on a regular basis by the Online Safety Leader (see Appendix – monitoring log)

- Designated Safeguarding Leads will be informed of any Online Safety incidents involving Child Protection concerns (via CPOMS), 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 learning 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.
- 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. At Delph Side we are committed to dealing appropriately with incidents of Online Safety, and will act on any incidents that occur outside school that affect the wellbeing of pupils or staff.

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. It is intended that incidents of misuse will be dealt with through normal behaviour procedures

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 Leaderr 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 Computing 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.

Online Safety Policy
June 2019

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 Community users 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 Appendices)

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. (See Appendix – Online Safety Group Terms of Reference)

The group will also be responsible for regular reporting to the *Governing Body / Directors*.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Lead) with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Date: June 2019

Written by: Mr Fyne
Review date: June 2010

Online Safety Policy
June 2019

Appendices

Online Safety Policy
June 2019