Anderton Primary School

Online Safety Policy

Created July 2015

Reviewed May 2017

School Vision

Our school provides a diverse, balanced and relevant approach to the use of technology.

Our children are encouraged to maximise the benefits and opportunities that technology has to offer.

Our school ensures that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.

Our children are
equipped with the skills and knowledge to use technology appropriately and responsibly

Our school teaches children how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment.

All users in our school community understand why there is a need for an Online Safety Policy.

Online Safety Champion

The online safety champion at Anderton primary School is the head teacher.

The role of the Online Safety Champion includes:

Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents.

Ensuring that the policy is implemented and that compliance with the policy is actively monitored.

Ensuring all staff are aware of reporting procedures and requirements should an Online Safety incident occur.

Ensuring an Online Safety Incident Log is appropriately maintained and regularly reviewed.

Keeping personally up-to-date with Online Safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).

Providing Online Safety advice/training for staff, parents/carers and governors.

Ensuring the, SLT, staff, children and governors are updated as necessary

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.

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school.

This data must be:

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

All data in our school must be kept secure and staff informed of what they can or can't do with data.

The person responsible for managing information is the head teacher.

Relevant staff know the location of data which is held centrally on SIMS.net. Data is appropriately managed by three key people: the office manager, the head teacher and the deputy head teacher.

All staff with access to personal data understand their legal responsibilities.

Data is **NEVER** handed out to a person who does not have legal responsibility for the child.

All staff are made aware that they should only use approved means to access, store and dispose of confidential data. Any document containing a child's details must be shredded.

Staff do not have remote access to school data.

The class teacher in the EYFS is allowed to have data relating to the EYFS profile on a school lap top and this may be used at home for assessment purposes. This is the only circumstance where data is allowed to be used outside of school. (See Child Protection and Safeguarding Policy.)

Data is backed up every night by the office manager.

Mobile Devices

Mobile Phones

Mobile phones may be used by school staff in private at break time or lunch time. Staff may make a call inside a classroom if the door is closed and no children are present. Alternatively staff may use a mobile phone in the head teacher's office or staff room.

Mobile phones are not allowed in toilet areas or cloakrooms.

Mobile phones must be kept out of sight of the children at all times and be in silent mode during curriculum time.

Visitors must switch off mobile phones before entering the school.

Children are **not** allowed to have mobile phones in school. In some cases a child may bring a phone because they are going elsewhere after school and the phone is needed. In this case the class teacher looks after the phone for the day and the phone is returned to an adult at the end of the day.

Staff can be contacted if necessary and these messages should only be checked at break and lunch times.

Parents can make contact and pass messages to children via the office manager.

Images should only be captured on a school camera or school ipad. (See Child Protection Policy)

Staff are not allowed to access the internet on a personal device using the school wi fi password

On school visits staff must only take the school camera or the school ipad.

School staff may use their own mobile phone when on school visits.

The dangers of Online bullying are taught in our school as part of the school's e Safety programme through assemblies and inviting in relevant visitors to speak about Online bullying.

Staff are vigilant in monitoring visitors for any covert use of mobile phones/ cameras.

Staff must report any misuse of a mobile phone to a member of the Senior Leadership Team.

Other mobile Devices

Use of digital media

(Cameras and recording devices)

Photographs and videos of children and adults may be considered as personal data in terms of The Data Protection Act (1998).

We obtain **written** consent from parents for photographs of their children to be taken or used. Parents give consent for photographs to be used on the school website, in the media, and in the school prospectus. Parents can consent to none, one or all of these options. (See Appendix 1)

Parents are informed of the timescale for which images will be retained. Permission is sought if a child's photograph is to be used after the child has left the school.

We ask for permission to take and use photographs every September at the start of the school year.

Parents must to inform us if they wish to withdraw consent for photographs.

Parents are informed of the purposes for which images may be taken and used e.g. displays, website, brochures, learning journeys and portfolios, press/other external media.

We seek specific parental permission for a child's images to be included in portfolios maintained by trainees/students not directly employed by the school. The trainee/student teacher must always ask permission of the class teacher before any photograph is taken.

In the event of a child's photograph being part of a group we seek permission from the other parents concerned before publishing a photograph.

The press have special permission in terms of Data Protection and may wish to name individual children to accompany a photograph. We seek parental permission for this.

Each class teacher keeps a list that shows which child has parental permission for photographs to be taken and for what purpose.

Taking Photographs/ Video

Staff members are entitled to take photographs or video of the children.

Students and trainees must ask permission of the class teacher to take photographs or video and must explain fully the purpose of this. Class teachers will seek advice from the online safety champion.

Only school owned equipment can be used to take photographs/video.

When taking photographs/video the rights of the child/adult to refuse to have their photograph taken are respected at all times.

Photographs will **NEVER** be used showing children or adults who may be upset, embarrassed or distressed in any way.

We will ensure that a range of children are shown in photographs for publication purposes and will do our best not to favour the same children.

We will carefully consider the angle of photographs before using photographs showing PE activities.

Photographs will never be taken in toilets or cloakrooms.

Close up shots will be avoided as these may be considered intrusive. Photographs will preferably include a background context and show children in group situations.

Parents Taking Photographs / Videos

Under the Data Protection Act (1998), parents are entitled to take photographs of ***their own*** children on the provision that the images are for ***their own*** use.

Including other children for other purposes 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. This is communicated through newsletters.

Parents are reminded, in writing, that publishing images which include children other than their own or other adults on Social Network sites is not acceptable, unless specific permission has been obtained from the subjects.

Parents are reminded at the start of productions, plays and sports days to only photograph/video their own children.

Storage of Photographs / Video

Photographs are stored on T drive.

Images may be stored on school USB memory sticks but these are not allowed off the premises.

Staff are not allowed to store images on personal equipment

All staff apart from welfare staff have access to photographs /videos stored on school equipment.

Each class teacher is responsible for deleting images that have been taken during the school year. Photographs of children who have left the school are deleted.

If a parent withdraws permission for their child to be used for any purposes then the class teacher is informed and the child is removed from the consent list.

Photographs are sent by e mail in a secure way using a secure lancsngfl address.

Publication of Photographs / Videos

Consent is requested from parents for publication of children's images, e.g. on a website.

Photographs will only be published online to secure sites.

Full names and/or other personal information should not accompany published images. Only the child's first name will accompany a photograph if permission is given.

When publishing images

We communicate to staff via newsletters that photos of children other than their own should not be used on social networking sites.

Staff and children are made aware that full names and personal details will not be used on any digital media, particularly in association with photographs.

All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.

Staff ensure that personal profiles are secure and do not display content that is detrimental to their own professional status or could bring the school into disrepute.

The Media, 3rd Parties and Copyright

Third Parties such as the press are supervised at all times whilst in the school and we ensure that they comply with the Data Protection requirements in terms of taking, storage and transfer of images.

We agree not to send photographs to a third party to be used in any way.

Communication technologies

Email

All users have access to the Lancashire Grid for learning service as the preferred school email system.

Staff are allowed to use personal email accounts during school hours, on school equipment for professional purposes.

We have email accounts for children. These consist of one e mail address between two children and children cannot be identified. For example an e mail address in Year 3 uses the class name wiseowl1@anderton.lancs.sch.uk

Only official email addresses are used to contact staff.

All users are made aware of the risks of accessing content including SPAM, phishing, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.

All users are 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 are aware that email communications may be monitored at any time in accordance with the Acceptable Use Policy.

Children who e mail as part of a Computing topic, will be monitored closely by the class teacher. The children who learn how to send and receive e mail do so to a staff member in school only, using a lancsngfl address.

Users are made aware that they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act.

Websites and other online publications

The school website or online publication is effective in communicating Safety messages to parents/carers.

Everybody in the school is made aware of the guidance for the use of digital media on the school website.

Everybody in the school is made aware of the guidance regarding the inclusion of personal information on the website.

There are only three staff members allowed to access and edit the school website. These are the office manager, the head teacher and the HLTA.

The head teacher has overall responsibility for what appears on the school website.

Downloadable materials are in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re- distributed without the school's consent.

Infrastructure and technology

Our school ensures that the infrastructure/network is as safe and secure as possible. We subscribe to the Lancashire Grid for Learning and therefore filtering is provided by default. It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included in the school's subscription, and must be installed on computers in school and configured to receive regular updates.

Further information can be found at
www.lancsngfl.ac.uk/esafety.

Children's access

Children are supervised at all times when using school equipment to access online materials.

Key stage 2 children have access to the school systems through individual and/or class logins

Children's access is restricted to certain areas of the network.

Adult access

Access to school systems is available for staff and is restricted according to their areas of responsibility. (See safe use acceptance sheets in the Internet Policy.)

Passwords

Staff are made aware of the guidelines in the Lancashire ICT Security Framework for Schools. This is available at **www.lancsngfl.ac.uk/esafety** website.

All users of the school network have a secure username and password.

The administrator password for the school network is kept secure and is only available to the head teacher, the office manger and the technical support service.

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

Staff are prompted through lancsngfl to change their password for the network.

Software/hardware

The school has ownership of all software (including apps on tablet devices.)

An up to date record of appropriate licenses for all software is kept and the Computing Subject leader is responsible for maintaining this.

Equipment and software is audited regularly and placed on the asset register.

Blue Orange technical support and the Computing subject leader control the software that is installed on school systems.

Managing the network and technical support

Servers, wireless systems and cabling is securely located and physical access restricted.

All wireless devices have security enabled.

Wireless devices are accessible only through a secure password.

Relevant access settings been restricted on tablet devices e.g. downloading of apps or ‘inapp’ purchases.

Blue Orange technical services are responsible for managing the security of the school network.

The safety and security of the school network is reviewed annually.

Computers are regularly updated with critical software updates/patches.

Users (staff, children, guests) have clearly defined access rights to the school network e.g. they have a username and password.

Staff and children are reminded to 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. Only Blue Orange technical support can do this.

Users must report any suspicion or evidence of a breach of security to the online safety champion or the Computing subject leader. The head teacher has overall responsibility.

A school USB device may be used outside of school on a school device

A school laptop must not be used for personal use.

All internal/external technical support providers are aware of the schools requirements /standards regarding online safety.

The Computing subject leader is responsible for liaising with/managing the technical support staff?

Filtering and virus protection

The school has requested devolved control over the LGfL filtering service.

The filtering system is managed and by the Computing subject leader.

Devolved filtering is communicated to all members of staff through CPD.

All staff are aware of the procedures for blocking and unblocking specific websites.

Procedures are in place to ensure that ALL equipment including school laptops used at home are regularly updated with the most recent version of virus protection software used in school.

Staff are aware of the procedures for reporting suspected or actual computer virus infection.

Dealing with incidents

Our school has considered the types of incident that may occur and how these will be dealt with. An incident log (see Appendix 2) will be completed to record and monitor offences. This will be audited on a regular basis by the Online Safety Champion or other designated member of the Senior Leadership Team.

Illegal offences

Any suspected illegal material or activity will be brought to the immediate attention of the head teacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF)

We will never personally investigate, interfere with or share evidence as we may inadvertently be committing an illegal offence.

We will 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

More details regarding these categories can be found on the IWF website **http://www.iwf.org.uk**

Inappropriate use

The table below shows areas of inappropriate use which may arise and sanctions that are in place.

Incident	**Procedure and Sanctions**
Accidental access to inappropriate materials.	Minimise the webpage/turn the monitor off/click the 'Hector Protector' button. Tell a trusted adult. Enter the details in the Incident Log and report to LGfL filtering services if necessary. Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously Deliberate searching for inappropriate materials Bringing inappropriate electronic files from home. Attempting to use chat rooms and forums in an inappropriate way.	Inform SLT or designated Online Safety Champion. Enter the details in the Incident Log. Additional awareness raising of Online Safety issues and the AUP with individual child/class. More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. Consider parent/carer involvement.
Using social media sites inappropriate at home to contact staff members or to bring the schools name into disrepute.	Parents informed Online safety talk given by the head teacher, class teacher and the police informed if necessary .

In this school the head teacher is responsible for dealing with e Safety incidents. The head teacher is the Online Safety champion and is also the DSP (Designated Senior person) for Child Protection.

All staff are made aware of the different types of Online Safety incident and how to respond appropriately.

Children are kept informed as are parents of any Online Safety incidents and the outcomes.

Incidents are logged on an incident log sheet kept electronically in HT documents folder.

Parents are involved and invited in for discussions which include the child. Sanctions are explained and given at this meeting.

Procedures are in place to protect staff and escalate a suspected incident/allegation involving a staff member.

We consider the three main areas of Online Safety risk (as mentioned by OFSTED, 2013) as follows:

Area of Risk	Example of Risk
Content: Children need to be taught that not all content is appropriate or from a reliable source.	Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse. Lifestyle websites, for example proanorexia/ 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 using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Online bullying in all forms Identity 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 and others.	Privacy issues, including disclosure of personal information, digital footprint and online reputation Health and well-being - amount of time spent online (internet or gaming). Sexting (sending and receiving of personally intimate images). Copyright (little care or consideration for intellectual property and ownership – such as music and film).

Online Safety - Across the curriculum

We provide regular, planned online Safety teaching within a range of curriculum areas using the Lancashire ICT Progression document.

Online Safety education is progressive throughout the school and all children regardless of additional needs are included.

We regularly discuss online Safety in assemblies and in PSHE.

Children are made aware of the impact of online bullying and know how to seek help if they are affected by these issues.

Children know to talk to a trusted adult. (See Anti Bullying Policy - children's' version)

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

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 of school. Children are regularly reminded of the safe use of online practices.

Children are reminded of safe Internet use through classroom displays and online Safety rules.

Online Safety – Raising staff awareness

Staff are made aware of online safety updates through CPD. These can be planned or incidental.

The Lancashire online Safety officer will provide a more formal awareness briefing on an annual basis for all staff.

Online Safety training ensures that staff are made aware of issues which may affect their own personal safeguarding for example the use of Social Networking sites.

All staff are expected to promote and model the responsible use of ICT and digital resources.

Online Safety training is provided within an induction programme for all new staff, to ensure that they fully understand both the school's Online Safety Policy and Acceptable Use Policy.

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).

We raise awareness to parents through: School newsletters, homework diaries, the school website and other publications.

Bespoke online Safety awareness sessions for parents are held on a regular basis.

We promote external online Safety resources/online materials through online Safety presentations, newsletters and the school website.

Raising Governors' awareness

Governors, particularly those with specific responsibilities for Online Safety, ICT or Child Protection, are kept up to date through discussions at Governors' Meetings, attendance at Local Authority Training, or internal staff/parent meetings.

Appendix 1

Anderton Primary School

PARENTAL CONSENT FORM

Dear Parent

During the school year we may take photographs of the children at our school. These images may be used in our school prospectus, other printed publications that we produce on the school website, or on a projected display board in school. We are sometimes visited by the media who will take photographs of pupils (e.g. at a high profile event, to celebrate a particular achievement etc.) Such images may appear in local or national newspapers.

In order to comply with the Data Protection Act 1998, we need your permission before we can photograph your child for promotional purposes. Equally, we are committed to continue to work closely with parents in an attempt to take all reasonable steps towards making the school environment as safe as possible.

Please answer questions 1 – 3 below before returning the completed form (one for each child) to school as soon as possible.

		(Please tick) Yes	No
1.	May we use your child's photograph in the school prospectus and other printed publications that we produce for promotional purposes, including community and links with other schools	☐	☐
2.	May we use your child's image on our school website?	☐	☐
3.	Are you happy for your child's photograph and first name only to appear in the media as part of schools involvement in an event?	☐	☐

I have read and understand the conditions of use on the back of this form.
Child's Name: _____

Signature: _____Parent or Guardian

Name_____
(Block capitals please)

Date: _____

Conditions of Use

1. This form is valid from the date upon which you sign it, for the period of time your child attends this school. Your consent will automatically expire after this time.

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

3. The school will not include personal e-mail, postal addresses, telephone or fax numbers on our website, in our school prospectus or in other printed publications.

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

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

6. We may include pictures of pupils and teachers that have been drawn by pupils.

7. We may use group or class photographs with very general labels such as 'science lesson'.

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

9. Parents who are invited to attend events where photography is permitted in school should ensure that any images or materials produced are for family/private use only.

10. Parents should take note that websites can be viewed throughout the world.

11. We undertake to take all reasonable steps to ensure that any images maintained in school are stored securely and are accessed only by authorised persons.

Signed:_____

Mrs L Minton Head teacher

Appendix 2

Online Safety Incident Log

Date /Time of Incident	Type of Incident	Name of pupils/Staff involved	System details	Incident details	Resulting actions taken and by whom