Online Safety Policy
2026

Introduction

This policy applies to all members of the Seven Stars Primary School and Nursery community (including staff, pupils, parents / carers, visitors and school community users).

Research has proven that use of technology can brings great benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

Our school's vision for Online Safety

Our school provides a diverse, balanced and relevant approach to the use of technologies, especially as the children move further up the school.

Children are encouraged to maximise the benefits and opportunities that technology has to offer including various recording technologies, iPads, use of cloud storage and continued use of desktop computers.

As a whole staff we ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.

All the children throughout school are aware of the SMART rules. Following these rules ensures that children are equipped with the skills and knowledge to use technology appropriately and responsibly; thus becoming a good digital citizen.

School does teach how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment in IT (Purple Mash), PSHE lessons. The focus should be on managing risk not blocking it out altogether; giving the children strategies for use in later life and being positive in their behaviours online.
All users in our school community understand why there is a need for an Online Safety.

The role of the school's subject leader for computing

The Head teacher and School Business Manager are in charge of the school website and also periodically tracks use of different websites and use of images etc. on i-Pads and computers with the support of the BTLancs IT support team and reporting arrangements.

The Head teacher is the nominated point of contact within the school for Online Safety related issues and incidents. However, certain responsibilities may need to be delegated to other staff e.g. the IT subject leader or the Designated Senior Person/Child Protection Officer as is necessary.

The role of the Online Safety Champion should include:

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

- Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Ensuring any Online Safety Incident is logged and reported to the appropriate person
- Keeping personally up-to-date with Online Safety issues and guidance through liaison with the Local Authority Schools ICT Team and website and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP). This will be updated on the school website and reported to parents where relevant.
- Providing or arranging Online Safety advice/training for staff, parents / carers and governors.
- Ensuring the Head teacher, SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person / Child Protection Officer.

Security and data management

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

And importantly, only transferred to others with adequate protection.

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

Use of mobile devices:

Tablets, pen drives, mobile phones, I-Pads, Digital Cameras, Voice recording devices, etc.

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

- That some mobile devices e.g. mobile phones, game consoles or net books can access unfiltered internet content. If Wi-Fi is enabled on the device, this device can be found by others outside of the school community
- That any devices used outside of school are virus checked before use on school systems
- Children are taught to use apps in a responsible manner appropriate to age and task

Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

As photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act, school must have written permission for their use from the individual and/or theirparents or carers. **See Appendix 2.**

A form or 'opt out' must be sent to parents as their children enter school to ensure we have permission from them to use their child's image and ensure that consent is given by staff or parents who are likely to appear in any photographs/video.

Staff and pupils are aware that full names and personal details will not be used on any digital media, particularly in association with photographs. Children's first name and surname together will never be used on the website, Twitter or blog. The Class Dojo platform is a closed systems between school and the parent of the child.

Parents /carers, who have been invited to attend school events, are allowed to take videos and photographs, but are asked not to publish them online or on personal websites where anyone can view them.

All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites and are asked to keep their pages private and not available for public viewing.

Staff should use school cameras, i-Pads or a school mobile phone to take pictures of the children and will ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.

All staff, parents / carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved through the curriculum and E Safety advice for parents which is accessible on the school website and in monthly e-Safety newsletters.

Communication technologies

In our school the following statements reflect our practice in the use of email.

It is recommended that all users have access to the Lancashire Grid for Learning service as the preferred school e-mail system.

Our IT technician visits school fortnightly and is able to set up new accounts for both staff and pupils. Only official email addresses should be used to contact parents / pupils – personal accounts should be discussed with the knowledge of the head teacher.

The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts.
Any incidents of repeated SPAM should be reported to the subject leader.
All users are aware of the risks of accessing content including SPAM, 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 and the Freedom of Information Act, meaning that safe practice should be followed in respect of record keeping and security.

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

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

Our school includes a standard disclaimer at the bottom of all outgoing emails: 'The views expressed in this e-mail are entirely those of the sender and do not necessarily represent the views of our school...'

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

The use of social networking sites has over recent years become the primary form of communication between friends and family.

In addition, there are many other sites which allow people to publish their own pictures, text and video. Social Network sites allow users to be part of a virtual community. Current popular examples of these are Tik Tok, Facebook, Threads, You Tube, Instagram and X.

Sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user.

As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments. It is widely acknowledged that use of such sites does not provide a completely private platform. Even when utilized sensibly and with caution, employees cannot control comments or

images published by others which may portray the employee in a manner which is not conductive to their role in school.

All staff need to be aware of the following points – These will be highlighted in regular staff meetings over the year:

- They should not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites. No online 'friendships' are made whilst employed by school as this could lead to professional relationships being compromised.
- Any adult employed by Seven Stars Primary School and Nursery must not communicate with pupils using any digital technology where the content of the communication may be considered inappropriate or could be misinterpreted.
- If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.
- Dating sites will never be accessed in school – examples include Match.com, Tinder, Zoosk.
- Staff should not use social networking sites to 'vet' prospective employees. Such practice could potentially create an un-level playing field and lead to claims of discrimination.
- Current pupils should **never** be added as 'friends' on any Social Network site. It is unwise to add past pupils, particularly under the age of 18.
- Children are taught to use blogs appropriately and to speak on them as they would face-to-face with anyone.
- Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web, it is available for everyone to see and remains there forever.

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

Mobile phones are not automatically permitted in school for children's use. Should a child ever have a mobile phone in school (e.g. because they are walking home after school and parents want to be able to contact them) then the child should hand in their mobile phone at the start of the day to the class teacher / staff member who will keep them out of the way and secure. They will then have them returned by a member of staff at the end of the school day. Mobile phones should not be used on the school premises by pupils.

Staff should ensure their own phones are turned off/ silent during lessons and not used during lessons or in front of children. They can only be used in the staffrooms and office areas.

Lots of children wear watches and they are great for helping children to learn how to tell the time but please be advised that children should not bring smart watches into school. This means any watch with capabilities to take photographs or be used to send/receive messages or make phone calls will be treated as if a phone was brought in. If a child wears such a watch to school, it must be collected from the main office by an adult at the end of the school day.

Children can wear a digital, analogue or fitness watch, such as these:


They must not wear a smart watch, such as these:

Text messages are sent out to parents via Class Dojo to give notification of club times and messages. Parents are encouraged to message the school office on Class Dojo or by phoning school to report absences.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Instant Messaging:

This is a popular tool used by adults and pupils that allows 'real time' communication and often integrates the ability to transmit images via a webcam.

Staff and children are aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

Lots of work and constant updates occur on our school website and on Class Dojo. As a staff, we will ensure that our school website is effective in communicating Online Safety messages to parents / carers. (SMART rule updates on each class page)

It is made clear there are to be no pictures linked to full names.

Content is always considered subject to copyright/personal intellectual copyright restrictions and all information on our school website is available for everybody to see.

Most downloadable materials from the school website are in a read-only format (e.g. PDF) where necessary, to reduce the likelihood of content being manipulated and potentially re distributed without our school's consent.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing:

The relevant permissions letter is made available for parents / carers to sign giving permission for their child / children to participate in video and photographs.

Children should never be appearing 'live' on the Internet through a video conferencing link without a member of staff present at all times.

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. Face time calls should never be used on staff mobile phones on the school premises.
Approval by the Head teacher must be obtained in advance of the video conference taking place.

All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with broadcastings.

An example of when this may be very helpful is when a child is on long term illness, but well enough to view lessons and keep in contact with his peers.

Acceptable Use Policy (AUP)

As attached as Appendix 3 and signed copies to be kept with the Head teacher.

Dealing with incidents

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Online Safety leader who will then log and pass on to Head teacher who must refer this to external authorities, e.g. Police, CEOP, and Internet Watch Foundation (IWF).

We will never personally investigate, interfere with or share evidence as we may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident (http://www.iwf.org.uk). These groups 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

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. Some examples of inappropriate incidents are listed below with suggested sanctions.

Incident Procedure and Sanctions

Accidental access to inappropriate materials:

- Minimise the webpage/turn the monitor off then tell a trusted adult.
- Enter the details in the school 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:

- Inform the leadership team and the IT Co-ordinator.
- Enter the details in the Incident Log which is kept locked away in the Leadership Room.
- Raising awareness 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

Deliberate searching for inappropriate materials:

- Inform the Leadership Team or the IT Co-ordinator.
- Enter the details in the Incident Log.
- Raising awareness 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.
- Bringing inappropriate electronic files from home.
- Consider parent / carer involvement.

Infrastructure and Technology

As a school, we are responsible for ensuring that your infrastructure /network is as safe and secure as possible.

Pupil Access:

Pupils can only log onto a computer with their domain user name and password. Administrator passwords are changed yearly.

Passwords:

All the year group passwords and admin passwords are kept by the IT Co-ordinator.

Software/hardware:
Our IT Co-ordinator regularly updates computers and checks hardware.

Managing the network and technical support:

The IT Co-ordinator has access to further support from Lancashire Digital Education Services.

Filtering and virus protection:

All our computers are Sophos protected and are monitored through LGfL. We now have devolved filtering using the Net sweeper system and staff can ask for websites to be 'unblocked'. This is done by a form kept with the Subject leader. Face Book will not be unblocked. You Tube is for classroom teaching purposes only and is only accessible with an adult domain username and password.

Education and Training

Education and training are essential components of effective Online Safety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and how to deal with them is fundamental. Online Safety guidance must be embedded within the curriculum and advantage taken of new opportunities to promote Online Safety. This can be done through discreet IT lessons or PSHE. Please refer to the Computing Policy and Computing Coverage Overview to see how this is applied in school.

Online Safety Across The Curriculum

All staff are expected to promote and model responsible use of IT and digital resources. Regular updates on Online Safety Policy, Acceptable Use Policy, curriculum resources and general Online Safety issues are discussed in staff meetings.

Online Safety – Raising staff awareness

All staff are made aware of this policy through our staff handbook. Updates are added to relevant staff meetings.

Online Safety – Raising parent's/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).

Our school offers regular opportunities for parents / carers and the wider community to be informed about Online Safety, including the benefits and risks of using various technologies through notes for parents on the website and monthly e-safety updates which are e-mailed to the whole school community. Teachers also give appropriate advice where appropriate.
There is also external agencies' advice on our website, which is regularly checked for relevance.

Online Safety – Raising Governors' awareness

Governors are to be made aware of this policy and any updates via governor meetings. An Online Safety link governor will also need to be named and work alongside our safeguarding governor.

Standards and inspection

Since September 2009 there has been greater emphasis on monitoring safeguarding procedures throughout schools.
As a school we should consider on a regular basis:

- How will we know if our Online Safety policy is having the desired effect?
- How are Online Safety incidents monitored, recorded and reviewed?
- Who is responsible for monitoring, recording and reviewing incidents?
- Is the introduction of new technologies risk assessed?

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

APPENDIX 1

Image Consent Form

Name of Child: _____ Year Group: _____

We regularly take photographs / videos of children at our school. These may be used on Class D0jo, our school prospectus, in other printed publications, on our school website, on social media such as Twitter or Facebook or in school displays.

Occasionally, our school may be visited by the media who will take photographs/ videos of an event or to celebrate a particular achievement. These may then appear in local or national newspapers, websites or on televised news programmes. Children's full names will never appear with their picture unless parents are consulted on specific occasions. Pictures of children in swim suits or similar clothes will never be taken.

In order that we can protect your child's interests, and to comply with the Data Protection Act (1998), please read the Conditions of Use, complete, sign, date and return this form (one for each child) as soon as possible.

Conditions of Use

1. This form is valid for your child's time at this school.
2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.
3. The school will not use the personal contact details or full names (which means first name and surname) of any pupil or adult in a photographic image, or video, on our website / social media or in any of our printed publications.
4. If we use photographs of individual pupils, we will not use the full name of that pupil in any accompanying text or caption.
5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.
6. We will only use images of pupils who are suitably dressed and not seen to be in a compromising position.
7. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.
8. This form replaces any previous correspondence.

Consent

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

I give permission for my child's image in ALL the ways identified above.

OR

I would only like my child's image to be used in the following ways: (Please list)

Parent / Carer signature: _____

Name (PRINT): _____ Date: _____

APPENDIX 2 - ICT Acceptable Use Policy (AUP) – Staff and Governor

Agreement

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

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

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

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

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

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

6. I will respect copyright and intellectual property rights.

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

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

9. I will not install any hardware or software without the prior permission of the IT Co-ordinator or Senior Leadership.

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

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

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

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

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

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

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

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

18. I will help pupils to be safe and responsible in their use of ICT and related technologies.

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

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

Full name and role..... (PRINT

APPENDIX 3 - Child Friendly Acceptable Use Policy

Internet and Computer Safety Rules

(Acceptable Use)

1. **Respect Yourself**
   - I will show respect for myself through my actions.
   - I will only use websites for my schoolwork.
   - I will ask a teacher before using a game site.
2. **Respect Others**
   - I will use words that are respectful and kind. No bullying!
   - I will let my teacher know if I see something inappropriate on the computer.
   - I will only change or modify other's work with permission.
   - I will act responsibly and take good care of school computers and equipment (clean hands, gentle keyboarding, two hand carry, etc.)
3. **Protect Yourself**
   - I will keep my personal information private.
   - I will not share my password or login information.
   - I will report people who try to bully me to a trusted adult.
4. **Protect Others**
   - I will be an ally to others and report any bullying or inappropriate behavior to a trusted adult.
   - I will not change settings and preferences on the computer.
5. **Respect Copyright**
   - I will not download or use words, pictures, video or music that are protected by copyright.
   - I will cite my sources.

I pledge to protect myself and my friends.

_____

(First and Last Name)