



Balderstone St Leonard's CE Primary School

Online Safety Policy

August 2026

For Online Safety

To provide a balanced and relevant approach to the use of new technologies.

To allow children to maximise the benefits and opportunities that technology has to offer.

To ensure appropriate security that is balanced with the need to learn effectively.

To ensure children are equipped with the skills and knowledge to learn effectively.

To teach children about the risks associated with technology and how to deal with them both within and outside the school environment.

To keep up to date with the latest Online Safety information.

To ensure children feel confident to talk about their online world and issues that affect them.

Use Of Mobile Devices

Mobile phones

Children are not allowed to bring mobile phones into school.

If a mobile phone is brought into school staff will remove it from the child and keep it safe until the end of the day.

Staff may bring mobile phones into school for personal use but these must be switched off during teaching sessions. (they may only be switched on in exceptional circumstances, e.g an emergency). If a member of staff needs to have their phone on during the day, they must leave it in the office with Mrs Oddie.

Staff may use their mobile phones in the staff room or once all children have left the building at the end of the day.

Staff may carry their own mobile phones when taking children off site on educational visits. This is for emergency contact.

Staff must not use their personal phones to take pictures, videos or make recordings of children.

Other Mobile Devices

School cannot be held liable for damage to or the loss of any mobile device brought into school.

Use Of Digital Media (cameras and recording devices)

Written Parental consent is gained for the use of any photographs taken in school and this is communicated to all staff.

Photographs of children and school events can be taken by any member of staff who should only use school equipment.

When taking photographs staff should respect the dignity and rights of the individuals.

Staff are responsible for ensuring images are stored responsibly and that they are deleted once they are no longer needed.

The class IPAD must be passcode protected and only the class teacher should access it.

Photographs held on the IPAD must be used and deleted as soon as possible.

Photographs that are being stored for curriculum evidence should only be on the class teachers lap top or class ipad. These may be kept until the end of the academic year in which they are taken.

The class teachers lap top and ipad must be password protected.

It is recognised that teachers may need to work with photographs at home. Photographs should only ever be stored on a school password protected device.

PHOTOGRAPHS OF CHILDREN MUST NEVER BE TAKEN ON ANY PERSONAL OR MOBILE DEVICE THAT BELONGS TO A MEMBER OF STAFF.

PHOTOGRAPHS OF CHILDREN MUST NEVER BE DOWNLOADED ONTO DEVICES OR PC'S THAT STAFF HAVE AT HOME.

PARENTS ARE REQUESTED NOT TO TAKE PHOTOGRPHS ON THEIR PERSONAL DEVICES AT SCHOOL EVENTS. EVERY EFFORT WILL BE MADE TO SHARE PHOTGRAPHS WITH PARENTS.

Publication Of Images.

Consent is gained from parents for publication of images.

When images are published care is taken to ensure that individual children and adults cannot be identified. No personal information accompanies published images.

Staff must ensure that when using social networking personal profiles are secured and that they do not display content that is detrimental to their own professional status or that could bring the school into disrepute.

CCTV, video conferencing, VOIP and Webcams

Parents will be informed if CCTV, video conferencing or webcams are to be used in school.

All video conferencing sessions will be logged.

Communication Technologies

All staff have access to the Lancashire Grid for learning service as the schools preferred email system.

All emails may be monitored at any time in accordance with the acceptable use policy.

Social networks.

The use of social networking sites such as Facebook, Bebo, X and MySpace is common for communication between friends and family. In addition there are many sites which allow people to publish their own pictures, text and videos such as You Tube and Instagram.

Careful use of these sites should have no impact on the professional role of staff in school.

However use of these sites does not provide a completely private platform for personal communication.

To protect themselves, staff should follow the guidance below:

Staff must not access these sites for personal use during working hours.

Content on Social Network sites may be unmediated and inappropriate for certain audiences.

If a Social Network site is used personally, details must not be shared with children and privacy settings should be reviewed regularly to ensure information is not shared with a wider audience than intended.

Content posted online must not :-

- Bring the school into disrepute
- Lead to valid parental complaints
- Be deemed derogatory towards the school and/or its employees.
- Be deemed derogatory towards pupils and/or parents and carers.
- Bring into question their appropriateness to work with children or young people.

Staff should not form online friendships with parents/carers or pupils (including ex pupils) as this could lead to professional relationships being compromised.

Staff must not give personal contact details to parents/carers including mobile telephone numbers.

Adults must not communicate with children using any digital technology where the content of the communication may be considered inappropriate or misinterpreted.

Staff should not communicate online with parents, past pupils or siblings of pupils. An exception is email communication with parents from school email addresses.

Children or parents must not be added as "friends" on any social networking site.

Instant Messaging

Staff must not use school equipment to communicate with personal contacts.

School Website

There is a dedicated Online Safety section on the school website under the Curriculum area of computing.

The website content is managed by the Headteacher.

All staff who have access to edit the website are aware of Online considerations.

All downloadable materials must be uploaded in PDF format.

Infrastructure And Technology

Children can access the school system within lessons. The school system is filtered and security protected.

Children have access to their own file on the curriculum network in which to store their work.

Staff access to school systems is restricted according to areas of responsibility.

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

An update register of all hardware is kept.

An up to date record of all licenses for software is kept.

Software is installed by the school technician.

Managing the network and technical support.

The curriculum network is managed by the Headteacher in conjunction with technical support from Micro Computer Consultants Ltd.

The school has a yearly contract for technical support.

Dealing With Incidents

Any suspected illegal material or activity must be brought immediately to the attention of the Headteacher who has to refer this to the external authorities.

Never personally investigate, interfere with or share evidence as you may be inadvertently committing an illegal offence.

Inappropriate Use

Any inappropriate use should be reported to the Headteacher.

A log of any inappropriate use will be kept and monitored by the Headteacher.

All staff and children sign an acceptable use policy (AUP).

A programme for E-safety that ensures information for parents, training for staff and regular E-Safety teaching is in place.

Monitoring Internet Use

Updated in line with Keeping Children Safe in Education 2019. Advice sought from Graham Lowe, Online safety adviser, Lancashire Safeguarding Children's Board. Updates from the uk safer internet centre.

Children never have unsupervised use of the internet in school.

The opportunities for children to access the internet should be planned and closely monitored.

Children should never be allowed to use search engines randomly.

Children will be taught how to use appropriate search engines in a responsible manner.

Teachers will plan and direct children to suitable websites.

Children will be regularly reminded that they must speak out if the notice anything online that causes concern.

Class teachers will keep a log if any Online Safety concerns in the class behaviour log files. These will be monitored half termly by the SLT.

As part of their yearly contract MCC will monitor the Log Files.

They provide a summary to the Headteacher of sites that have been blocked by filtering.

The Headteacher will follow up any incidents causing concern

E-Safety Across The Curriculum

The school will run activities during national E-Safety Awareness Week in addition to regular reminders in computing and PSHE lessons about keeping safe online.

The children are made aware of the impact of cyberbullying and how to seek help.

They are taught to critically evaluate materials and develop good research skills through cross-curricular teaching and discussion.

Children are reminded of safe internet use through posters displayed in school.

Parents are reminded about the eSafety section on the school website

Safeguarding Issues

Communicating with both current and former pupils via social networking sites or via other non-school related mechanisms such as personal e-mails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

DFE Safeguarding guidance states:

- All staff should sign an Acceptable Use policy (AUP).

- The E-Safety policy should be reviewed on an annual basis.
- Adults should ensure that pupils are never listed as approved contacts on any social networking site.
- Adults should never access the social networking sites of pupils.
- Adults should never give personal contact details to pupils, including their mobile phone number.
- Adults should only make contact with children for professional reasons.
- Adults should not use the internet or web-based communication channels to send messages to a child

Disciplinary action may be taken in relation to those members of staff who choose not to follow the advice and guidance outlined in this policy.