**For the love of learning, friendship and faith**

**Melling St Wilfrid CE Primary School**
**Internet Access and Online Safety Policy**

## Introduction

This Internet Access Policy outlines how Internet use supports the educational aims of our School. This policy will be reviewed on an annual basis.

The purpose of Internet Access at our School is to raise educational standards, to support professional work and to enhance the school's management information and business administration systems. School Internet use is increasing and it is becoming an important part of learning and communication across all curricular areas and is an invaluable tool in the development of lifelong learning skills.

Children and teachers at our School have access to a range of online materials that enrich and extend teaching and learning opportunities.

The benefits to teaching and learning include:
✔ Access to world-wide educational resources including museums and art galleries;
✔ Information and cultural exchanges between pupils nationally and world-wide;
✔ Assess to news and current affairs;
✔ Access to educational materials and learning resources;

Internet access is an entitlement for pupils based on responsible use. Children will be taught from an early age that they are responsible for their actions on the internet.

Internet access will be carefully planned to enrich and extend learning opportunities as an integrated aspect of the curriculum. Pupils will be given clear objectives for Internet use and will access material under guidance from their class teacher. Teachers will supervise pupils and take all reasonable precautions to ensure that users only access material appropriate to their learning. Parents are informed that pupils will be provided with internet access to support their learning and parents are required to sign a Parental Consent Form.

**Internet use**

The school's Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of information location, retrieval and evaluation. When appropriate the school will use 'safer' search engines and online resources to support pupils in locating and retrieving information.

At Melling St Wilfrid CE Primary School, we:

- ✔ Encourage pupils to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable or they recognise as inappropriate.
- ✔ Ensure pupils and staff know what to do if they find inappropriate web material i.e. to switch off the computer and report the URL to the headteacher.
- ✔ Teach pupils how to evaluate Internet content and to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- ✔ Teach Online Safety
- ✔ Deliver a rolling training programme of support to parents who have an important role in supporting safe and effective use of the Internet by pupils.
- ✔ Ensure pupils and staff know what to do if a cyber-bullying or other safety incident occurs (please also see our anti-bullying policy).

**Managing Internet Access and Information system security**

At Melling St Wilfrid CE School, we:

- ✔ Maintain broadband connectivity.
- ✔ Ensure virus protection is updated regularly.
- ✔ Use class and individual log-ins for pupils.

We use the Lightspeed filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature. Staff and students are aware that they must report any failure of the filtering systems directly to the headteacher. Our headteacher will report this to the Governing Body on a termly basis.

At Melling St Wilfrid CE Primary School, we:

✔ Block all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.

✔ Only use approved discussion sites/approved Learning Platforms and block others.

✔ Only use approved or checked webcam sites.

## Authorising Internet access

✔ All pupils and staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

✔ Parents will be asked to sign and return a consent form for their child attending the school.

## Email

✔ Pupils can only use the email accounts prepared for them on the school system.

✔ Pupils are introduced to, and use email as part of the ICT scheme of work.

## Images

✔ Digital images /video of pupils are stored in the teachers' shared images folder on the network

✔ Digital images are not stored on staff memory sticks or home technology.

✔ We do not use pupils' names when saving images in the file names.

✔ We do not include the full names of pupils in the credits of any published school produced video materials / DVDs.

✔ Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.

✔ Pupils are taught about how images can be abused in their eSafety education programme.

✔ We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.

## Using the School Network and System

This school:

✔ Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet and email access and can be given an individual network login username and password.

✔ Provides pupils with a class or individual network login username and password.

✔ Makes it clear that staff must keep their login username and password private and must not leave them where others can find.

✔ Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network.

✔ Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles.

✔ Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.

✔ Requires all users to always log off when they have finished working or are leaving the computer unattended.

✔ Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.

✔ Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used solely to support their professional responsibilities.

✔ Ensures that our wireless network is managed securely and only staff are aware of the wireless password. Use of the wireless network for personal use is not permitted.

## Safeguarding guidance for staff with reference to online communication

Communication between pupils and adults should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, emails, digital cameras and social networking sites. Communicating with both current and former pupils via technology can lead to employees being vulnerable to serious allegations concerning safeguarding of children and young people. Staff at our School are requested to:

✔ Ensure that personal social networking sites are set as private and pupils are never listed as approved contacts.

✔ Never use or access social networking sites of pupils.

✔ Do not give their contact details to pupils including in their mobile number

✔ Familiarise themselves with LCC GUIDANCE ON THE USE OF SOCIAL NETWORKING SITES AND OTHER FORMS OF SOCIAL MEDIA policy.

## Online Safety

The Green Paper *Every Child Matters* and the provisions of the *Children Act 2004 Working Together to Safeguard Children* sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

At our School, we recognise our duty to ensure that every child in our care is safe, and believe the same principles apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

**The Technologies**

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://wwwlivewire.com/)
- Mobile phones with camera and video functionality
- Smartphones with email, web functionality and cut down 'Office' applications.

**Whole school approach to the safe use of ICT**

Creating a safe ICT learning environment includes three main elements:
- ✔ An effective range of technological tools
- ✔ Policies and procedures, with clear roles and responsibilities
- ✔ A comprehensive Online Safety policy for pupils, staff and parents

**Roles and Responsibilities**

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and monitored. She ensures that she is up to date with Online Safety issues and guidance through liaison with the Local Authority Online Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP). The Headteacher ensures the Governors are updated as necessary. Governors need to have an understanding of Online Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on Online Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

- ✔ All staff should be familiar with the schools' Policy including:
- ✔ Safe use of e-mail;
- ✔ Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- ✔ Safe use of school network, equipment and data;
- ✔ Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- ✔ Publication of pupil information/photographs and use of website;
- ✔ EBullying / Cyber Bullying procedures;
- ✔ Their role in providing Online Safety education for pupils;
- ✔ Staff are reminded/updated about Online Safety matters at least once a year.

**How will complaints regarding Online Safety be handled?**

The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or

mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible consequences:

- Discussion with Online Safety Coordinator / Headteacher
- Informing parents or carers
- Removal of Internet or computer access for a period
- Referral to LA / Police

Our Headteacher acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA safeguarding/child protection procedures.

**Monitoring and Review**

This Policy has been approved by the Governing Body and will be reviewed annually in consultation with school staff. The policy is available to parents and the wider community. The Online Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection. The Online Safety Policy and its implementation will be reviewed annually.

**Internet Access and Online Safety Policy**

Date: September 2020

Signed (Headteacher): F Ip

Signed (Governing Body representative): M Jackson

Review date: September 2021