LITTLE MISSENDEN CE INFANT SCHOOL

E SAFETY POLICY

I. Introduction

1.1   Writing and reviewing the e-safety policy

- This e-Safety Policy has been written by building on the Bucks e-Safety Policy and government guidance. It has been agreed by staff and approved by the governing body.
- The school has appointed an e-Safety Coordinator who is also the Designated Child Protection Co-ordinator (Michelle Green).

2 Teaching and learning

2.1.1 Why the Internet and digital communications are important

- The Internet is an essential element of life today for education, business and social interaction.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Our school provide pupils with internet access as part of their learning experience.
- As pupils use the internet widely outside school they need to learn how to take care of their own safety and security.
- The use of the internet in school is to raise educational standards, including pupil achievement and to support the professional work of staff.

2.1.2 How does internet use benefit education?

Benefits of using the internet in education include:

- Access to worldwide educational resources and learning including museums and art galleries.
- Professional development for staff through access to educational materials and effective classroom practice.
- Collaboration across networks of schools, support services and professional associations.
- Exchange of curriculum and administration data with Bucks County Council.

2.1.3 Internet use will enhance learning

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to infant age pupils to enhance and extend education.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.
- Staff will guide pupils to online activities that support their learning outcomes.
- Pupils will be educated in the effective use of the internet including navigation.
- Pupils will be shown how to publish and present information to a wider audience.

2.1.4 Pupils will be taught how to respond to unpleasant content

friendship, thankfulness, honesty, forgiveness, compassion and trust

- Pupils and staff will be taught to report unpleasant internet content to the Head teacher who will then contact the network support team to have the site filtered.

2.2 Managing Internet Access

2.2.1 Published content and the school web site
- Staff or pupil personal contact information will not generally be published.
- The contact details on the website are the school address, email and telephone number.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.2.2 Publishing pupil's images and work
- All parents or carers sign forms on entry giving or with-holding permission for photographs to be published on the school Web site or in the media.
- Pupils' full names will not be used anywhere on a school Web site or other online space, particularly in association with photographs.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic devices.

2.2.3 Social networking and personal publishing
- We do not allow social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, e-mail addresses, full names of family/friends, specific interests and clubs.
- Parents will be advised that the use of social network spaces outside school brings a range of dangers for infant aged pupils.
- Parents and staff are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff will adhere to the rule that any friend request from a child or parent in their school must NOT be accepted. Equally no staff should request friendship with a current pupil or parent.

2.2.4 Managing filtering
- The school will work with the Bucks County Council, and the school's support team to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Head teacher.
- Staff will ensure that annual checks are made to ensure that the Bucks County Council and the school's support team's filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF (internet watch foundation) or CEOP.

2.2.6 Managing emerging technologies
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

friendship, thankfulness, honesty, forgiveness, compassion and trust

- The staff should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time (see the Use of Mobile Phones Policy). The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The school has a mobile phone policy regarding staff use of personal phones
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

2.2.7 Protecting personal data
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.3 Policy Decisions
2.3.1 Authorising Internet access
- All staff must read and sign the "Staff Code of Conduct for ICT" before using any school ICT resource.
- Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form when pupils enter the school.
- Any person not directly employed by the school will be asked to sign an "acceptable use of school ICT resources" before being allowed to access the internet from the school site.

2.3.2 Assessing risks
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Buckinghamshire County Council can accept liability for any material accessed, or any consequences resulting from of Internet use.

2.3.3 Handling e-safety complaints
- Complaints of Internet misuse will be dealt with by the Headteacher or Chair of Governors. Staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- All e-safety complaints and incidents will be recorded by the school – including any actions taken.

2.3.4 Community use of the Internet
- The school will be sensitive to internet related issues experienced by pupils out of school.

2.3.5 How will cyberbullying be managed?
Cyberbullying (along with all forms of bullying) will not be tolerated in school. At the time of writing this policy, no cyberbullying has ever been reported at Little Missenden C of E Infant School. However, should an instance occur, the following will take place:

friendship, thankfulness, honesty, forgiveness, compassion and trust

- Support for anyone affected by cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying possible witnesses, and contacting the service provider if necessary.
- Sanctions for those involved in cyberbullying may include:
    The bully will be asked to remove any material deemed to be inappropriate or offensive
    Service provider may be contacted to remove content.
    Internet access may be suspended at school for the user for a period of time.
    Parent/carer may be informed.

2.4 Communications Policy

2.4.1 Introducing the e-safety policy to pupils
- E-Safety rules are discussed with pupils at the beginning of each academic year, with frequent reminders.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- e-Safety training will be embedded within the Computing scheme of work or the Personal Social and Health Education (PSHE) curriculum covering both safe school and home use.

2.4.2 Staff and the e-Safety policy
- All staff and governors will be given the School e-Safety Policy and its importance explained.
- To protect all staff and pupils, the school will implement acceptable use policies.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

2.4.3 Enlisting parents' and carers' support
- Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Information and guidance for parents on e-safety will be made available to parents in a variety of formats.

The public sector equality duty of the Equality Act 2010 has been considered in the writing of this policy. A Discrimination Impact Assessment concludes that through this policy Little Missenden C of E Infant School seeks to:
- **Eliminate discrimination, harassment and victimisation and other conduct prohibited by the Act.**
- **Advance equality of opportunity between people who share a protected characteristic and those who do not.**
- **Foster good relations between people who share a protected characteristic and those who do not.**

Protected Characteristics: age, disability, gender, gender identity, race, religion or belief, and sexual orientation.

friendship, thankfulness, honesty, forgiveness, compassion and trust

Useful resources for teachers
Please refer to the DfCSF e-safety policy guidance for further information.

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/

Becta
http://schools.becta.org.uk/index.php?section=is

Chat Danger
www.chatdanger.com/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org/
Bucks e-Safety Policy and Guidance, Posters etc

Kidsmart
www.kidsmart.org.uk/
Bucks Police – e-Safety

Think U Know
www.thinkuknow.co.uk/

Safer Children in the Digital World www.dfes.gov.uk/byronreview/

friendship, thankfulness, honesty, forgiveness, compassion and trust

Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD
http://publications.teachernet.gov.uk

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com

friendship, thankfulness, honesty, forgiveness, compassion and trust

Appendix 3: E-Safety Audit – Primary / Special

This self-audit should be completed by the member of the Team responsible for the e-safety policy annually.

	Response	Action required	Action completed
Has the school got an e-Safety Policy that complies with BCC guidance?			
Date of latest update (at least annual).			
Date the school e-safety policy was agreed by governors.			
The policy is available for staff in the policy folders in school.			
The policy is available for parents/carers on the school website.			
Name of the responsible member of the Leadership Team.			
Name of the responsible member of the Governing Body.			
Name of the Designated Child Protection Coordinator.			
Name of the e-Safety Coordinator.			
Has e-safety training been provided for both pupils and staff where appropriate?			
There a clear procedure for a response to an incident of concern.			
E-safety materials from CEOP and Becta been obtained if appropriate.			
All staff sign a Code of Conduct for ICT on appointment.			
All pupils aware of the School's e-Safety Rules.			
Parents/carers sign and return an agreement that their child will comply with the School e-Safety Rules. (Code of Conduct)			
Staff, pupils, parents/carers and visitors are aware that network and Internet use is closely monitored and individual usage can be traced.			
Has an ICT security audit been initiated by SLT, possibly using external expertise?			
If personal data is collected, stored and used is this according to the principles of the Data Protection Act?			
Internet access provided by an approved educational Internet service provider which complies with DCSF requirements (e.g., Regional Broadband Consortium, NEN Network).			
The school-level filtering been designed to reflect educational objectives and approved by HT.			

friendship, thankfulness, honesty, forgiveness, compassion and trust

friendship, thankfulness, honesty, forgiveness, compassion and trust