HYNDBURN PARK PRIMARY SCHOOL
ONLINE SAFETY POLICY

1. INTRODUCTION

Online Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

2. IMPORTANCE OF TECHNOLOGY AND ONLINE SAFETY

At Hyndburn Park Primary School we recognise that technology has a clear role to play in supporting, enhancing and providing key skills in children's learning. The curriculum requires pupils to learn how to locate, retrieve, exchange and present information using a range of technologies. Web based resources are vital to access life-long learning and employment; indeed the use of technology is now seen as an essential life-skill.

Usually, the resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the internet, by its very nature, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at all times, they will be able to move beyond these, to sites unfamiliar to the teacher.

Staff in our school will plan to integrate the use of technology for the benefit of our pupils. Most technologies present risks as well as benefits. In line with school policies that protect pupils from other dangers, we endeavour to provide our pupils with as safe an internet environment as possible and teach them to be aware of and respond responsibly to any risks.

Vigilance and supervision are our key strategies. In accordance with Lancashire County Council policy we will take all reasonable steps to ensure that pupils are not placed in an embarrassing or potentially harmful situation. Pupils, staff, parents / carers, and adult helpers are all asked to play their part in assisting pupils to use the internet responsibly and safely (see appendix 1 for a flowchart to respond to Online Safety incidents, along with an example of the incident form to be used following any Online Safety incidents).

3. AUTHORISED INTERNET ACCESS

- The school will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the 'Acceptable Use Agreement' (appendix 2) before using any school technological resources. This will be completed annually, at the beginning of each academic year.
- Parents will be informed that pupils will be provided with supervised internet access.
- Parents will be asked to sign and return a consent form for pupil access (see appendix 3). This will be completed at the start of the school journey. Parents / carers of children who join the school at any other point throughout the year will complete the pupil access form as part of the admission arrangements.
- Internet use will be supervised as we do not believe that pupil's browsing the web in an undirected way is educationally productive.

- Pupils will be taught to use the internet responsibly in accordance with both our school and Lancashire County Council Policy guidelines. They will be expected to adhere to the Acceptable Use Policy. Pupils will receive guidance on what to do if they come across inappropriate material.

4. EMAIL

Pupils in Year 1 – 6 will be provided with an email address through the school email system (RM Unify). The use of this is restricted to pupils, teachers and support staff only. This email facility does allow children to send or receive email from outside the school system i.e. through the link on the school website however pupils are taught acceptable use during computing lessons. Our school email is subject to monitoring.

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a member of staff if they receive offensive e-mail (see appendix 1).
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

5. USE OF MOBILE DEVICES

- Under the Data Protection Act 1998, the school seeks parental consent to take photographs and use video recorders. Photographs will be stored in year group folders on the server. All computers are password protected.
- The schools digital cameras, iPads or memory cards must not leave the school setting unless on an official school trip. Photos are printed / uploaded at school by staff and once completed images are then immediately removed from the camera's memory.
- Photographs may be taken on school premises or on official school trips / visits / outings. Printed off photographs will be displayed on display boards or in children's books. Often photographs may contain other children in the background.
- Consent is gained from all parents / carers for children's work, photographs and videos to be used.
- All parents / carers of children who join Hyndburn Park Primary School in nursery / Foundation Stage sign a permission form which considers the use of photographs via the website or in school. Up-to-date consent forms are acquired for all children.
- Recording / photographing events such as sports day, outings/trips, Christmas and fundraising events by parents / carers will only be carried out for personal use. No photographs / recorded events are to be shared online.
- If any events require photographing / recording then named staff members will be asked to undertake this using school equipment.
- The majority of members of staff own a mobile 'phone. Many of these 'phones have inbuilt cameras. During the day mobile 'phones need to be switched off. Members of staff may use their mobile 'phones during break and / or lunch times as long as no children are present. If a member of staff is expecting urgent news, then permission should be sought to leave the 'phone on from the headteacher or member of the school's Leadership Team acting in her absence.
- If personal mobile phones are automatically synced to access work related e-mails, they must be password protected.
- **Cameras and mobile phones are prohibited in all toilet and changing areas.**

6. SOCIAL NETWORKING

- All social networking sites and newsgroup sites are blocked / are filtered unless specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils will be advised not to place personal photos on any social network space.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others.

7. FILTERING

- The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible. The school technician monitors the effectiveness of the filter regularly. The anti-virus protection (Symantec Endpoint Protection) is added to each computer and laptop throughout school, with an automatic update taking place at a specified time each day. Security strategies will be discussed with the Internet Service Provider (RM Unify).
- The school also use eSafe to monitor online activity.

8. PUBLISHED CONTENT AND THE SCHOOL WEBSITE

- The contact details provided on the website are the school address, e-mail, telephone and fax number. Staff or pupils' personal information will not be published.
- The headteacher / Website leader (and school technician) will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Class teachers will have an up to date list of children who are not allowed to have their photograph taken or be recorded on film. It is the responsibility of the teacher to ensure photographs and recordings are not put on our website..

9. PUBLISHING PUPILS' IMAGES AND WORK

- Photographs that include pupils will be selected carefully and will be cross-referenced with the pupil access record to ensure children without permission do not appear on the website.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents / carers will be obtained before photographs of pupils are published on the school website (see appendix 3).
- Work will only be published with the permission of the pupil and parents (see appendix 3).

10. SECURITY AND DATA MANAGEMENT

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- All data at Hyndburn Park will be kept secure and staff informed of what they can or cannot do with the data.

- All computers and laptops in school are password protected. The use of personal pen drives is not permitted, and any pen drives that are used must be encrypted (provided to each member of teaching staff). Visitors are made aware of the requirements and as such the named member of staff will ensure that all procedures are followed. For example, if a visitor would like to share a PowerPoint presentation, this must be emailed to the named member of staff prior to the visit in order to check content and ensure external pen drives are not used.

11. ASSESSING RISKS

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Lancashire County Council can accept liability for the material accessed, or any consequences of internet access.
- The school audits use of technology to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

12. EDUCATION AND TRAINING

- In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond.
- Online Safety is threaded throughout the computing curriculum across the whole school. Each computing session covers an aspect of Online Safety to ensure this is embedded.
- In order to raise the awareness of Online Safety with all stakeholders, the following training sessions have been undertaken:

Training provided for	Nature of training	Date
Pupils	• Safer Internet Day • Cyberbullying • Online Safety assemblies (Infants and Juniors) *Online Safety is also threaded throughout the computing curriculum across the whole school.*	• 12.02.13,11.02.14, 10.02.15, 09.02.17 • 18.11.13 – 22.11.13 • 06.02.13, 07.02.13, 05.02.14, 06.02.14, 12.02.14, 13.02.14, 21.01.15, 22.01.15
Parents / Carers	• Parents' evenings Online Safety workshop for parents / carers • Staying Safe Online information shared	• 31.03.14, 20.10.14, 19.10.15, 24.10.16, 21.03.17. • 09.03.15,12.11.15, 17.10.16, 13.06.17 • 27.02.15, 12.05.17
Staff	• Child Protection and Safeguarding	• 03.09.13, 04.09.14, 04.09.15, December 2015, 01.09.16, weekly inputs in staff meetings.

	• Anti-bullying / cyber bullying staff meeting • Curriculum development • Using iPads in the classroom • Online Safety workshop for staff • New curriculum for Online Safety.	• 04.11.13, 10.11.14 • 23.06.14 • 26.01.15 • 09.03.15, 30.01.17 • 12.06.16
Governors	• Termly meetings with the lead governor for CP&S • Online Safety update training.	• 27.03.17, 05.06.17

Annual training will take place for each group.

13. HANDLING ONLINE SAFETY COMPLAINTS

- Complaints of internet misuse will be dealt with by a member of the school's senior leadership team.
- Any complaint about staff misuse **must** be referred to the headteacher.
- 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.

14. COMMUNICATION OF POLICY

Pupils

- Rules for internet access will be posted in all networked rooms (appendices 4 and 5).
- Pupils will be informed that internet use will be monitored.
- Pupils will complete the acceptable use policy at the beginning of each academic year outlining the role they will play in maintaining Online Safety at school.

Staff

- All staff will be familiar with the Online Safety policy and its importance.
- Staff are aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents / Carers

- Parents' attention will be drawn to the Online Safety policy in newsletters, the school brochure and on the school website (accessed at www.hyndburnpark.lancs.sch.uk).

15. RELATED POLICIES

The school's Online Safety policy will operate in conjunction with the following policies:

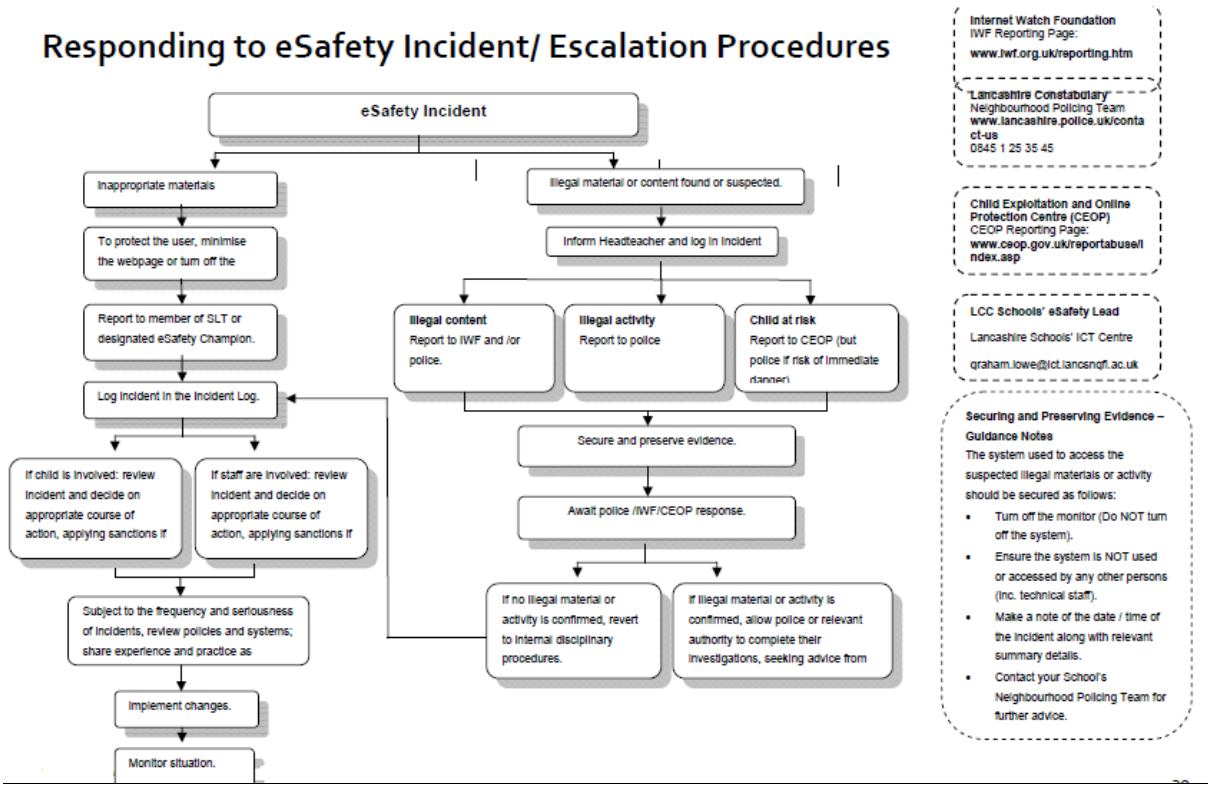
- Safeguarding and Child Protection;
- Guidance on Safe Practice for All Staff;
- Behaviour and Discipline;
- Anti-Bullying; and

- Teaching and Learning.

Updated:

Saiqa Tabsim: October 2012
Joanne Hardwick: September 2016
September 2017
September 2018
September 2019

APPENDIX 1 – FLOWCHART TO USE WHEN RESPONDING TO ONLINE SAFETY INCIDENTS



APPENDIX 2 – ACCEPTABLE USE POLICY FOR STAFF

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Online Safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school ICT subject leader or the Designated Safeguarding Person (DSL) for Safeguarding and Child Protection.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote Online Safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system maybe being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.
Signed: …… Name: ……
Date: ……
Accepted for school: …… Designation: ……

APPENDIX 3 – ONLINE SAFETY CONSENT FORM (PARENTAL PERMISSION)

All pupils use computer facilities including Internet access as an essential part of learning. Both pupils and their parents/carers are asked to sign to show that the Online Safety rules have been understood and agreed.

Name of Pupil: _____ *Class:* _____

Pupil's Agreement

- I have read and I understand the school Online Safety rules.
- I will use the computer, network, internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Pupil's Signature: _____ *Date:* _____

Consent for Web Publication of Work and Photographs

I agree that my child's work may be electronically published. I also agree that appropriate images and video that include my child may be published subject to the school rule that photographs will not be accompanied by pupil names.

Consent for Internet Access

I have read and understood the school Online Safety rules and give permission for my child to access the internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities. I understand that the school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

Parent / Carer Signature: _____ *Date:* _____

Use of Digital Images – Photography and Video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your child.

I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, for example on the school website, and for no other purpose.

I **do / do not** give my permission for my child to be photographed in school.

I **do / do not** give my permission for my child to be filmed in school.

Parent / Carer Signature: _____ *Date:* _____

APPENDIX 4 – RULES FOR INTERNET / COMPUTER USE ((CHILDREN)

When using the Internet you need to be . . .

S – Keep Safe

Don't give out your personal information.

Keep your full name, address, mobile number, email address, school name and friends' full names secret. Otherwise people can use this information to find and speak to you.

M – Don't meet up

Never meet up with an online friend.

Never arrange to meet an online friend; no matter how well you think you know the other person or however curious you may be.

A – Accepting Emails can be dangerous

Don't open junk mail.

Don't open emails from people you do not know or recognise.
If you open an email that says rude or unpleasant things, you must tell a trusted adult straightaway - and don't reply to it.

R – Reliable

Beware: people might not be who they say they are.

fun, but
ause you
ıg to.
u should
online.

- Tell Someone

ll an adult if you feel fortable or worried.

ards and chat rooms have an 'alert button' or an email address where you can tell the 'host' (who runs the board) that you're upset about something or someone.

Don't forget you can always log-off and leave the website.