Harrow Lodge Primary School

ONLINE SAFETY POLICY

REVIEWED:	**Autumn 2022**
APPROVED (T&S):	**Spring 2023**
EFFECTIVE PERIOD:	**Spring 2023-Spring 2024**
DUE FOR REVIEW:	**Autumn 2024**
RESPONSIBLE PERSON(S):	**Mrs T Price**

SIGNED BY CHAIR OF GOVERNORS ____________________

This policy is linked to the following mandatory school policies: Child Protection, Health and Safety, Home–School agreements, and Behaviour/Pupil discipline (including the Anti-bullying) policy.

1. INTRODUCTION

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

1.1 Computing covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Skype and Facetime
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

1.2 Whilst exciting and beneficial both in and out of the context of education, much computing, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

2. RATIONALE

2.1 We believe that children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the Internet and other technologies.

This document will serve as a guide for staff and a reference for parents, governors and other adults.

2.2 At Harrow Lodge Primary School, we have adopted a three-tier approach to online-safety:

2.2.1 Awareness – ensuring staff, children and adults are aware of the risks;

2.2.2 Education – providing staff, children and adults with the knowledge they need to protect themselves and others;

2.2.3 Technology – implementing systems to protect everybody at Harrow Lodge Primary School.

3. WHAT ARE THE RISKS?

3.1 The Byron Review has classified the risks as relating to **content, contact** and **conduct.** The risks are often determined by **behaviours** rather than the technologies themselves.

	Commercial	**Aggressive**	**Sexual**	**Values**
Content (child as recipient)	Adverts Spam Sponsorship Personal Info	Violet/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting Personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

3.2 The four categories of risks outlined in top row of the above diagram form the basis for safeguarding our children. Indeed, our school Internet filtering system uses these categories when determining which sites are inappropriate. The filtering system is described in more detail in the next section.

4. THE INTERNET

4.1 The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

4.2 All use of the Internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

4.3 The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.

4.4 Staff will preview any recommended sites before use.

4.5 Raw image searches are discouraged when working with pupils.

4.6 If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

4.7 All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

4.8 Harrow Lodge Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

4.9 Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

4.10 The school does not allow pupils access to internet logs.

4.11 The school uses management control tools for controlling and monitoring workstations.

4.12 If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Head Teacher.

4.13 The school buys into the technical support service provided by the trust (Partnership Learning) and it is the responsibility of the school, by delegation to the ICT Support Team to ensure that all software is up-to-date and that Anti-virus protection is installed and kept up-to-date on all school machines. This includes laptops loaned to staff for use out of school.

4.14 Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor is it the network manager's responsibility to install or maintain virus protection on personal systems.

5. ONLINE SAFETY IN THE CURRICULUM

5.1 The school provides opportunities within a range of curriculum areas to teach about Online Safety.

5.2 Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button. Websites with information for parents and children regarding Online Safety are linked from the school website.

6. PASSWORD SECURITY

6.1 **All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety Policy.**

6.2 Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and MLE, including ensuring that passwords are not shared unless done so on a professional capacity.

6.3 In our school, all ICT password policies are the responsibility of our ICT Support Team and all staff and pupils are expected to comply **with** the policies at all times.

7. SOCIAL NETWORKING

7.1 At Harrow Lodge Primary School, we actively restrict access to social networking sites for children.

7.2 **Children:**

7.2.1 Most networking sites have a live chat facility, as well as unfiltered access to potentially inappropriate content. All access is prohibited.

7.2.2 We also ensure that children are taught about the risks associated with these sites in their computing lessons. Many children have access to social networking sites from home. It is therefore essential that they are aware of how to use such sites with care.

7.2.3 However, we do not tolerate children attempting to make contact with staff through Social Networking sites. Any child who attempts to do so will be reported to the administrators of the site and this may lead to them being banned from the site.

7.3 **Staff:**

7.3.1 Staff are permitted to use the school's Internet access in their own time for personal use.

7.3.2 Should staff feel that their privacy has been compromised by children on such sites outside of school hours, they should block the child(ren) involved using the appropriate tool on the site and report the incident to the site's administrators. The incident should also be reported to the Head teacher or in her absence, the Deputy Head teacher immediately. Further guidance for staff on using social media safely outside of school is included in Addendum 3 'Social Networking Guidance'.

8. MOBILE PHONES AND CYBER BULLYING

The school has a separate policy on the use of mobile technology, which appears at the end of this policy as Addendum 2.

9. MANAGING EMAIL

9.1 The use of email within most schools is an essential means of communication for both staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international.

9.2 We recognise that pupils need to understand how to style an email in relation to their age and good ‘netiquette. In order to fulfil the National Curriculum for computing pupils must have experienced sending and receiving emails. We use our computing scheme of work to teach the sending and receiving of emails.

9.3 The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

9.4 It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.

9.5 E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.

9.6 Staff sending emails to external organisations, parents or pupils are advised to cc. the Head Teacher, line manager or designated account (usually the office).

9.7 Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

9.8 Pupils have their own individual school issued accounts

9.9 The forwarding of chain letters is not permitted in school.

9.10 All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

9.11 Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

9.12 Staff must inform (Head teacher) if they receive an offensive e-mail.

9.13 Pupils are introduced to email as part of the Computing Scheme of Work.

10. SAFE USE OF IMAGES

10.1 Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

10.2 With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

10.3 Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

10.4 Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

11.5 Consent of adults who work at the school

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

11.6 Publishing pupil's images and work

11.6.1 On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site/ Social media page
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

11.6.2 This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time.

11.6.3 Pupils' full names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published.

11.7 Storage of Images

11.7.1 Images/ films of children are stored on the school's network.

11.7.2 Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head teacher.

11.7.3 Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.

11.7.4 ***Class teachers and Admin Staff*** have the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

12. CYBER BULLYING

12.1 At Harrow Lodge Primary School, we take cyber bullying very seriously. We define cyber bullying as:

*The **persistent** targeting of an individual or group of individuals by others through the use of technology – this includes:*

The use of Social Networking Sites to target children;
The use of Instant Messaging such as MSN to target children;
The use of mobile phones to send abusive or threatening messages;
The use of the Internet to post defamatory comments;
Hacking or cracking another person's profile on a website.

12.2 This list is not exhaustive and any behaviour deemed to be cyber bullying will be dealt with in accordance with the school's ant-bullying policy.

13. EQUAL OPPORTUNITIES

Pupils with additional needs

13.1 The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' Online Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

13.2 Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children and young people.

14. ROLES AND RESPONSIBILITIES

14.1 School

14.1.1 As Online Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

14.1.2 The named Online Safety co-ordinator in our school is the Head Teacher, Lynette Searle or in her absence, Michelle Browne the Deputy Head Teacher, who have been designated this role as a member of the senior leadership team. The ICT Subject Leader, shares this responsibility with the Head Teacher/Deputy Head Teacher.

14.1.3 This information is disseminated to all staff and it is their responsibility to be aware of who holds this post.

14.1.4 It is the role of the Computing subject leader to keep abreast of current issues and guidance through organisations such as LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet and keep the Head teacher, governors and staff fully updated through regular ongoing INSET.

14.1.5 **Online Safety skills development for staff**

14.1.6 New staff receive information on the school's acceptable use policy as part of their induction.

14.1.7 All staff have been made aware of individual responsibilities relating to the safe-guarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart Addendum 1.)

14.1.8 **Managing the school Online Safety messages**

14.1.9 We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used.

14.2 Parents

14.2.1 At Harrow Lodge Primary, we believe that Online Safety is not just a school issue, but an issue that will affect children and adults alike throughout every aspect of life.

14.2.2 We therefore ask that parents and guardians:

- Promote a culture of honest discourse with regard to the dangers of the Internet;
- Take all reasonable precautions when allowing their children/wards to access the Internet;
- Ensure that they are aware of the capabilities of their children/wards' mobile phones;
- Support the school in its ethos of promoting an Online Safety conscious environment.

14.2.3 In order to achieve this, we recommend that:

- Computers to which children have access are in a communal area of the home;
- The screen faces outward to prevent covert usage;
- Parental control software is installed;
- Monitoring systems are in place.

14.2.3 Online Safety is everyone's responsibility. We believe that by fostering a sensible approach at home and at school, we will be able to equip children with the skills they need to become responsible users of technology.

14.2.4 Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

14.2.4 Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website/Social network page)

14.2.4 The school disseminates information to parents relating to Online Safety where appropriate in the form of;

- Information and celebration evenings
- Handy easy read leaflets in addition to the main policy
- Website/ Learning Platform postings
- Newsletter items

15. MISUSE AND INFRINGEMENTS

15.1 **Complaints**

Complaints relating to Online Safety should be made to the Head teacher or in her absence, the Deputy Head teacher. The school will log the incident and will follow the flowchart that appears at the end of this policy under Addendum 1.

15.2 All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Head teacher, or in her absence, the Deputy Head teacher.

15.3 Deliberate access to inappropriate materials by any user will lead to the incident being logged, depending on the seriousness of the offence; investigation by the Head Teacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart Addendum 1.)

16. MONITORING AND REVIEW

16.1 The governing body of Harrow Lodge Primary School has the responsibility to monitor the correct implementation of this policy. The Head teacher will keep the governors informed through termly head teacher reports and through the annual safeguarding audit.

16.2 Review Procedure

16.2.1 There will be an on-going opportunity for staff to discuss with the Online Safety coordinator any issue of Online Safety that concerns them.

16.2.2 This policy will be reviewed every 2 years and consideration given to the implications for future whole school development planning.

16.2.3 The policy will be amended earlier if new technologies are adopted or Central Government change the orders or guidance in any way.

Harrow Lodge Primary School

Rainsford Way, Hornchurch, Essex RM12 4BP

Mrs L Searle
Head Teacher

Telephone: 01708 448187
office@harrowlodgeprimary.com

Staff, Governors and Visitors
Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff 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 or Computing Subject leader.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable 'by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of the Head Teacher or ICT subject leader.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head Teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support and promote the school’s Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ………………………………… Date ……………………

Full Name ……………………………….....................................(printed)

Job title ....

Harrow Lodge Primary School

Rainsford Way, Hornchurch, Essex RM12 4BP

Mrs L Searle
Head Teacher

Telephone: 01708 448187
office@harrowlodgeprimary.com

Dear Parents/Carers,

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much computing, particularly web-based resources, are not consistently policed. All users need to be aware of be aware of the range of risks associated with the use of these Internet technologies.

We address issues regarding Online Safety on a regular basis throughout our teaching.

The governors are very committed to safeguarding all the children in our care and we have reviewed and re-written our Online safety policy to bring it in line with government regulations, so that all users of technology at school are aware of the procedures involved.

This Acceptable Use of ICT Agreement is a summary of our Online Safety Policy which is available in full, on request from the school office or can be viewed on our school website.

Please read and discuss with your child the Online Safety rules overleaf and return this sheet signed by both you and your child to the school. If you have any concerns or would like some explanation please contact your child's class teacher.

We have set the deadline for the form to be returned by the .... **after which your child will not be able to use the internet at school until such time that the signed formed has been returned.**

We hope that parents are able to recognise this is only to protect your children and keep them safe and will therefore give our request their urgent attention.

Yours sincerely,
Mrs Lynette Searle Head Teacher
Pupil's name:

I have read, understood and agreed with the Rules for Acceptable use of ICT.

Signed ……………………………………………. (child)

Parent's/Carer's Consent for Internet Access

I have read and understood the school rules for Acceptable Use of ICT and give permission for my son / daughter to access the Internet in school. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.

I agree that should my son/daughter need to access the internet at home or anywhere else, that I will take all reasonable precautions to ensure he/she cannot access inappropriate materials and that he/she will use the computer in an appropriate manner.

Signed……………………..……………… (parent/carer) Date…………………………

Harrow Lodge Primary School

Rainsford Way, Hornchurch, Essex RM12 4BP

Mrs L Searle
Head Teacher

Telephone: 01708 448187
office@harrowlodgeprimary.com

Acceptable Use Agreement: Pupil Acceptable Use Agreement / Online Safety Rules

- I will only use ICT in school for school purposes.
- I will not tell other people my computer passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using technology because I know that these rules are to keep me safe.
- I know that my use of technology can be checked and that my parent/ carer contacted if a member of school staff is concerned about my Online Safety.

Name of Pupil: ....

Class of Pupil:

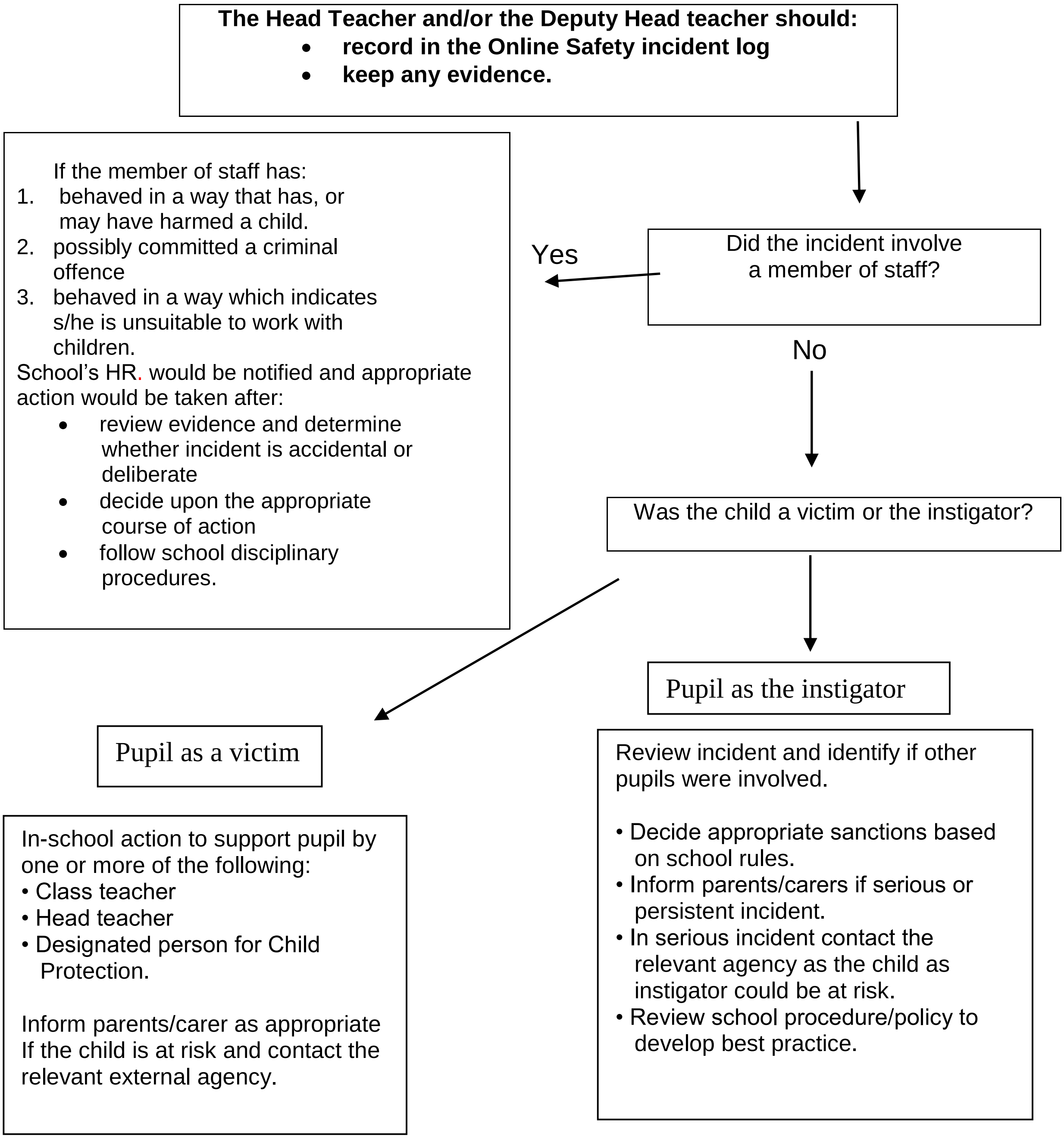
Signature of Pupil: ....

Flowchart for Managing an Online Safety incident not involving any illegal activity

Any member of staff witnessing any kind of Online Safety incident should report the matter to the Head Teacher or Deputy Head Teacher immediately.

This flowchart shows the way in which an Online Safety incident not involving any illegal activity will be managed by the school. These incidents may include:

- using another person’s user name and password
- accessing websites which are against school policy
- using a mobile phone to take video during a lesson
- using the technology to upset or bully (in extreme cases this could be illegal.)
-



The Head Teacher and/or the Deputy Head teacher should:

- **record in the Online Safety incident log**
- **keep any evidence.**

Did the incident involve a member of staff?

Yes

If the member of staff has:

1. behaved in a way that has, or may have harmed a child.
2. possibly committed a criminal offence
3. behaved in a way which indicates s/he is unsuitable to work with children.

School’s HR. would be notified and appropriate action would be taken after:

- review evidence and determine whether incident is accidental or deliberate
- decide upon the appropriate course of action
- follow school disciplinary procedures.

No

Was the child a victim or the instigator?

Pupil as a victim

In-school action to support pupil by one or more of the following:

- Class teacher
- Head teacher
- Designated person for Child Protection.

Inform parents/carer as appropriate If the child is at risk and contact the relevant external agency.

Pupil as the instigator

Review incident and identify if other pupils were involved.

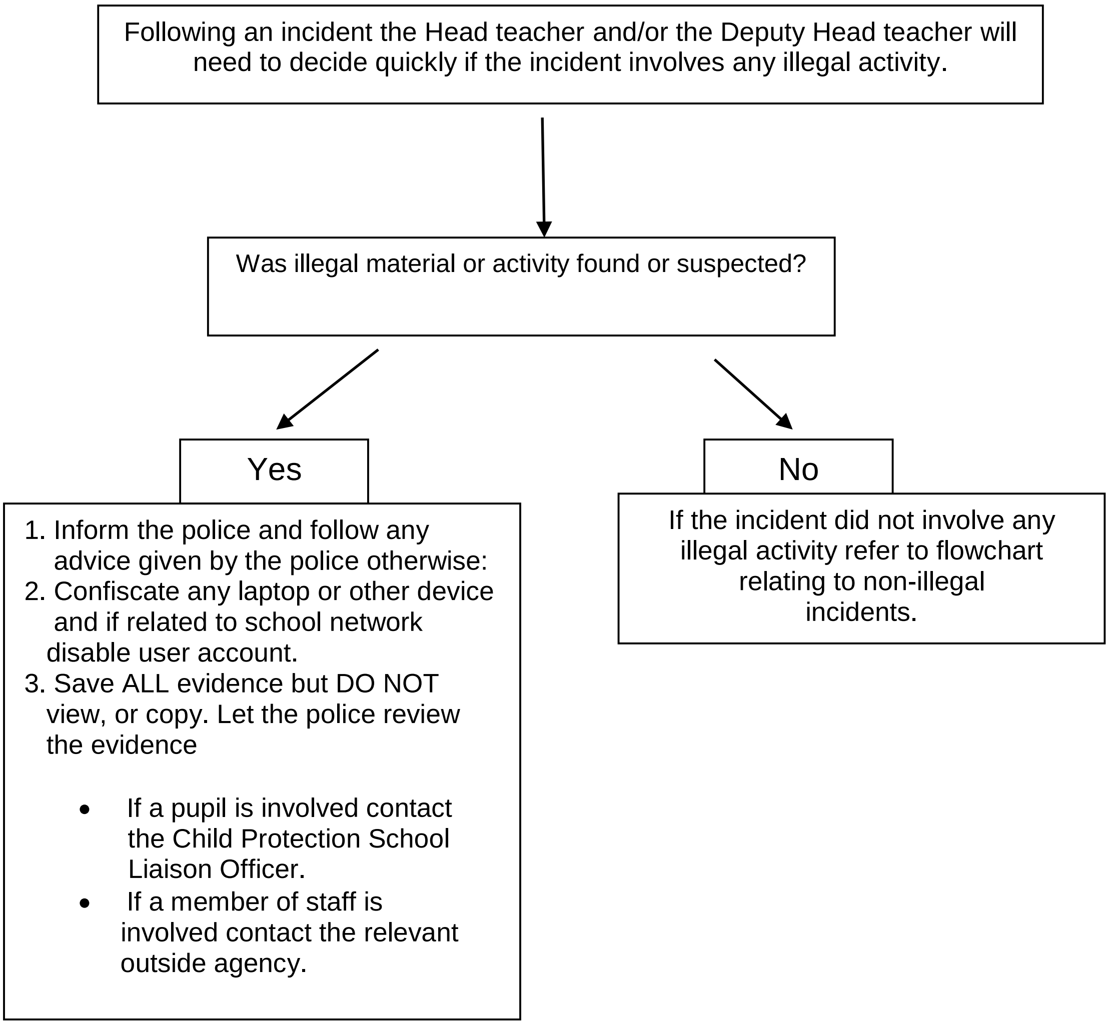
- Decide appropriate sanctions based on school rules.
- Inform parents/carers if serious or persistent incident.
- In serious incident contact the relevant agency as the child as instigator could be at risk.
- Review school procedure/policy to develop best practice.

Flowchart for Managing an Online Safety incident involving illegal activity

Any member of staff witnessing any kind of e-safety incident should report the matter to the Head Teacher or Deputy Head Teacher immediately.

This flowchart shows the way in which an e-safety incident involving any illegal activity will be managed by the school. These incidents may include:

- downloading child pornography
- passing onto others images or video containing child pornography
- inciting racial or religious hatred
- promoting illegal acts



Following an incident the Head teacher and/or the Deputy Head teacher will need to decide quickly if the incident involves any illegal activity.

Was illegal material or activity found or suspected?

Yes

1. Inform the police and follow any advice given by the police otherwise:
2. Confiscate any laptop or other device and if related to school network disable user account.
3. Save ALL evidence but DO NOT view, or copy. Let the police review the evidence

- If a pupil is involved contact the Child Protection School Liaison Officer.
- If a member of staff is involved contact the relevant outside agency.

No

If the incident did not involve any illegal activity refer to flowchart relating to non-illegal incidents.

Harrow Lodge Primary School
Online Safety Incident Log

Details of ALL Online Safety incidents to be recorded in the Incident Log. This Log will be kept by the Head Teacher. This incident log will be monitored termly by the Head Teacher and ICT Subject Leader.

Date & time	Name of pupil or staff member	Male or Female	Room and computer/device number	Details of incident (including evidence)	Actions and reasons

CURRENT LEGISLATION

Acts relating to monitoring of staff email Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of
"*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
For more information
www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.
-
The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited
by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing
written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Advice for Children on Cyber-bullying

If you're being bullied by phone or the Internet

- Remember, bullying is never your fault. It can be stopped and it can usually be traced.
- Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line.
- Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue.
- Don't give out your personal details online - if you're in a chat room, watch what you say about where you live, the school you go to, your email address etc. All these things can help someone who wants to harm you build up a picture about you.
- Keep and save any bullying emails, text messages or images. Then you can show them to a parent or teacher as evidence.
- If you can, make a note of the time and date bullying messages or images were sent, and note any details about the sender.

There's plenty of online advice on how to react to cyber bullying. For example,

www.kidscape.org and **www.wiredsafety.org** have some useful tips:

Text/video messaging
You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you've changed your phone number. To find out how to do this, visit

www.wiredsafety.org.

- If the bullying persists, you can change your phone number. Ask your mobile service provider.
- Don't reply to abusive or worrying text or video messages. Your mobile service provider will have a number for you to ring or text to report phone bullying. Visit their website for details.
- Don't delete messages from cyber-bullies. You don't have to read them, but you should keep them as evidence.
- Text harassment is a crime. If the calls are simply annoying, tell a teacher, parent or carer. If they are threatening or malicious and they persist, report them to the police, taking with you all the messages you've received.

Phone calls
If you get an abusive or silent phone call, don't hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off.

Once they realise they can't get you rattled, callers usually get bored and stop bothering you.

- Always tell someone else: a teacher, youth worker, parent, or carer. Get them to support you and monitor what's going on.
- Don't give out personal details such as your phone number to just anyone. And never leave your phone lying around. When you answer your phone, just say 'hello', not your name. If they ask you to confirm your phone number, ask what number they want and then tell them if they've got the right number or not.

- You can use your voicemail to vet your calls. A lot of mobiles display the caller's number. See if you recognise it. If you don't, let it divert to voicemail instead of answering it.
- And don't leave your name on your voicemail greeting. You could get an adult to record your greeting. Their voice might stop the caller ringing again. Almost all calls nowadays can be traced.
- If the problem continues, think about changing your phone number.
- If you receive calls that scare or trouble you, make a note of the times and dates and report them to the police. If your mobile can record calls, take the recording too.

Emails

- Never reply to unpleasant or unwanted emails — the sender wants a response, so don't give them that satisfaction.
- Keep the emails as evidence. And tell an adult about them.
- Ask an adult to contact the sender's Internet Service Provider (ISP) by writing to abuse@ and then the host, e.g. **abuse@hotmail.com**
- Never reply to someone you don't know, even if there's an option to 'unsubscribe'.
- Replying simply confirms your email address as a real one.

Web bullying

If the bullying is on a website (e.g. Bebo) tell a teacher or parent, just as you would if the bullying was face-to-face – even if you don't actually know the bully's identity. Serious bullying should be reported to the police - for example threats of a physical or sexual nature. Your parent or teacher will help you do this.

Chat rooms and instant messaging

- Never give out your name, address, phone number, school name or password online.
- It's a good idea to use a nickname. And don't give out photos of yourself.
- Don't accept emails or open files from people you don't know.
- Remember it might not just be people your own age in a chat room.
- Stick to public areas in chat rooms and get out if you feel uncomfortable.
- Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room.
- Think carefully about what you write; don't leave yourself open to bullying.
- Don't ever give out passwords to your mobile or email account.

Three steps to stay out of harm's way

- Respect other people - online and off. Don't spread rumours about people or share their secrets, including their phone numbers and passwords.
- If someone insults you online or by phone, stay calm – and ignore them.
- Think how you would feel if you were bullied. You're responsible for your own behaviour – make sure

Harrow Lodge Primary School

Addendum 2

USE OF MOBILE PHONE POLICY

DUE FOR REVIEW:	Autumn 2022
RESPONSIBLE PERSON(S)	MRS T PRICE

POLICY FOR PUPILS

Acceptable Use Policy for Mobile Phones - Y6 pupils only

1. PURPOSE

1.1. The widespread ownership of mobile phones among young people requires that school administrators, teachers, pupils, parents and carers take steps to ensure that mobile phones are used responsibly at schools. This Acceptable Use Policy is designed to ensure that potential issues involving mobile phones can be clearly identified and addressed, ensuring the benefits that mobile phones provide (such as increased safety) can continue to be enjoyed by our pupils.

1.2. Harrow Lodge Primary School has established the following Acceptable Use Policy for mobile phones that provides teachers, pupils, parents and carers guidelines and instructions for the appropriate use of mobile phones during school hours.

1.3. Pupils, their parents or carers must read and understand the Acceptable Use Policy before pupils are given permission to bring mobile phones to school.

2. RATIONALE

2.1. **Personal safety and security**
Harrow Lodge Primary School accepts that parents/carers give their children mobile phones to protect them from everyday risks involving personal security and safety. There is also increasing concern about children travelling alone on public transport or commuting long distances to school. It is acknowledged that providing a child with a mobile phone gives parents reassurance that they can contact their child if they need to speak to them urgently.

3. RESPONSIBILITY

3.1. It is the responsibility of pupils who bring mobile phones to school to abide by the guidelines outlined in this document.

3.2. The decision to provide a mobile phone to their children should be made by parents or carers.

3.3. Parents/carers should be aware if their child takes a mobile phone to school.

3.4. Permission to have a mobile phone at school while under the school’s supervision is contingent on parent/guardian permission in the form of a signed copy of this policy. Parents/carers may revoke approval at any time.

4. ACCEPTABLE USES

4.1**.** Mobile phones should be switched off upon arrival in the school grounds and handed to their class teacher.

4.2. All collected mobile phones will be locked away until the end of the day.

4.3 The school premises is not the place for pupils to be exchanging phone numbers, accessing the internet, sending messages or making calls to friends.

5. UNACCEPTABLE USES

5.1. Unless express permission is granted, mobile phones should not be used to make calls, send SMS messages, surf the internet, take photos or use any other application during school lessons and other educational activities, such as assemblies. Mobile phones may not be used at all by children on school grounds and may only be used by children on their journey to and from the school.

5.2 Guidance for parents and children on the safe use of mobile phones outside of school is available in the document 'Advice for children on cyber bullying'.

6. THEFT OR DAMAGE

6.1. Pupils should mark their mobile phone clearly with their names and hand them to the school office, as explained above.

6.2. Mobile phones that are found in the school and whose owner cannot be located should be handed to front office reception.

6.3**.** The school accepts no responsibility for replacing lost, stolen or damaged mobile phones.

6.4. The school accepts no responsibility for pupils who lose or have their mobile phones stolen while travelling to and from school.

6.5. It is strongly advised that pupils use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other pupils, or if stolen). Pupils must keep their password/pin numbers confidential. Mobile phones and/or passwords may not be shared.

6.6. Lost and stolen mobile phones in the U.K. can be blocked across all networks making them virtually worthless because they cannot be used.

7. INAPPROPRIATE CONDUCT

7.1. Any pupil who uses vulgar, derogatory, or obscene language while using a mobile phone will face disciplinary action as sanctioned by the head teacher.

7.2. Pupils with mobile phones may not engage in personal attacks, harass another person, or post private information about another person using SMS messages, taking/sending photos or objectionable images, and phone calls. Pupils using mobile phones to bully other pupils will face disciplinary action as sanctioned by the head teacher. [It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. As such, if action as sanctioned by the head teacher is deemed ineffective, as with all such incidents, the school may consider it appropriate to involve the police.]

8. SANCTIONS

8.1. Pupils who infringe the rules set out in this document (if phones are not handed in to the teacher or if the rules are broken before or after handing the phone in) will not be allowed to bring their mobile phone into school.

8.2. On the first infringement of this policy the mobile phone would be confiscated by the teacher and taken to a secure place within the school office. The student will be able to collect the mobile phone at the end of the school day and a record will be made of the incident. A letter will also be sent to the parent/carer to inform them of the incident. The location and form of the secure place will be one deemed appropriate by the management team.

8.3**.** On the second infringement the mobile phone would be confiscated by the teacher and taken to a secure place within the school office. Parents will be notified and the pupil will not be permitted to collect the phone without a parent/carer's consent. If a parent/carer is unable to attend the school, they are permitted to phone and give verbal consent for their child to collect the phone and must speak to a member of the management team or student support. The incident will be recorded.

8.4**.** On the third infringement the mobile phone would be confiscated by the teacher and taken to a secure place within the school office. Parents will be notified and the pupil will not be permitted to collect the phone without a parent/carer present. After the third infringement the school will withdraw the agreement to allow the student to bring the mobile telephone to school.

8.5. As set out in the previous section, failure to heed the rules set out in this document may result in an alleged incident being referred to the police for investigation. In such cases, the parent or carer would be notified immediately.

Harrow Lodge Primary School

Rainsford Way, Hornchurch, Essex RM12 4BP

Mrs L Searle
Head Teacher

Telephone: 01708 448187
office@harrowlodgeprimary.com

Parent/Guardian Permission

I have read and understand the above information about appropriate use of mobile phones at Harrow Lodge Primary School and I understand that this form will be kept on file at the school and that the details may be used (and shared with a third party, if necessary) to assist in identifying a phone should the need arise (e.g. if lost, or if the phone is being used inappropriately).

I give my child permission to carry a mobile phone to school and understand that my child will be responsible for ensuring that the mobile phone is used appropriately and correctly while under the school's supervision, as outlined in this document. I understand that my child must hand the phone in to their teacher when they arrive in class and the phone will not be available to them during the school day.

Parent name (print) ....

Parent signature ....

Date ....

Pupil's name (print) ....

Mobile phone number ....

Pupil's signature ....

Date ....

If you have any comments or suggestions, please write them in the box below.

POLICY ON THE USE OF MOBILE PHONES FOR STAFF

1. Staff use of mobile phones during their working school day should be:

- Outside of their contracted hours
- Discreet and appropriate e.g. Not in the presence of pupils.

2. At no stage whatsoever should a mobile phone be visible in the classroom or in teaching areas during contracted or teaching hours unless permission has been given by the headteacher.

3. Mobile phones should be switched off and left in a safe place during lesson time.

4. Staff should never contact pupils or parents from their personal mobile phone, or give their mobile phone number to pupils or parents. If a member of staff needs to make telephone contact with a pupil, a school telephone should be used.

5. Staff should never send to, or accept from, colleagues or pupils, texts or images that could be viewed as inappropriate.

6. With regard to camera mobile phones, a member of staff should never use their phone to photograph a pupil(s), or allow themselves to be photographed by a pupil(s).

7. This guidance should be seen as a safeguard for members of staff, the school and the Local Authority.

8. Staff should understand that failure to comply with the policy is likely to result in the enforcement of our Whistle-blowing policy and associated procedures.

Failure to comply with any of the above could be considered as breach of safeguarding.

Social Networking Guidance for Staff

Do not allow parents or children to add you as a friend, nor add them on friends on social networking sites such as Twitter or Facebook.

Do not use sites such as Facebook or Twitter whist at work.

Do not transmit any material that is likely to harass, cause offence, inconvenience or needless anxiety or to bring the school into disrepute.

Do not place any information regarding your activities in school or the school in general on your social networking sites (e.g. through status updates or posts on Facebook or Twitter).

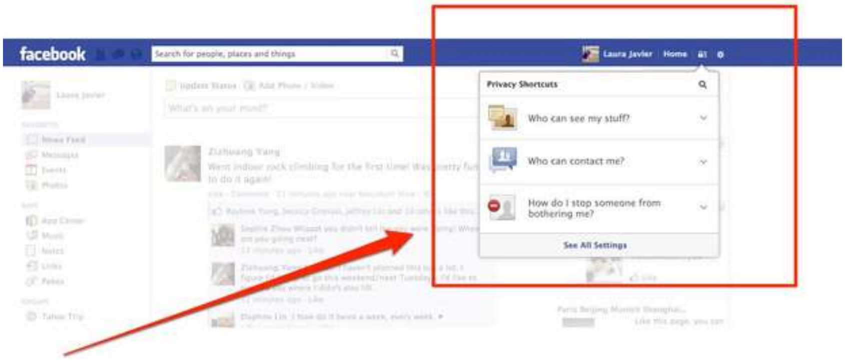
Take responsibility for your privacy on Social Networking sites. For example on Facebook you need to actively change your settings to ensure posts and photos are only available to friends.

If you use a social networking site such as Twitter or Pinterest as part of your Continued Professional Development to share resources and ideas with colleagues, then keep a separate professional and personal account.

Discussions about school matters should not be made using social networks (such as Facebook and Twitter) but should be made using School email accounts.

Facebook Security Settings

Social Networking site, Facebook updated its security settings in December 2012.



1) Log into your Facebook account.
2) Click on the padlock near the top-right side of the screen.
3) From this menu you can easily access your security settings.
4) Facebook tends to change the site design and security policy regulary, so it may be useful to keep an eye on your settings from time to time.

Classroom Displays

Online Safety at Harrow Lodge Primary School

To keep me safe whenever I use the internet, I promise…

- To keep my username and password private and not to use anyone else's.
- To keep all personal information private.

- To block unknown links and attachments by not opening anything that I do not trust.

- To report any messages or internet pages that are unsuitable or upsetting.

-To tell someone I trust if someone asks to meet me offline.

Online Safety Rules Key Stage 2

I will only open/delete my own files.

I will make sure that all contact made using technology to other children and adults is responsible, polite and sensible and will think carefully about how I talk to others online and what I say about them.

I will not deliberately look for, save or send anything that could be unpleasant or nasty. If accidentally find anything like this, I will tell my teacher immediately.

I will check that information I use from the internet is from a trusted website.

I will not give out my own details such as my name, phone number or home address.

I will be responsible for my behaviour when using technology because I know that these rules are to keep me safe.

I will not send any photos of myself or others without asking from permission from an adult and also the person/people who are in the photo.

I will not take, copy or send any images, video, sounds or text that could upset any member of the school.

I will only use chat and social networking sites that an adult has given me permission to use.

I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my Online Safety.

I will inform an adult if I see something that upsets me.

Online Safety Rules Key Stage 1

I will always ask an adult if I can use the computer, ipad, phone.

I will never give out my name, age, address or phone number to anyone online

I will never send photographs of myself unless I have asked an adult.

I will never agree to meet a stranger.

If I am allowed to use the computer, I will only open and change my work.

I will tell an adult if I see something I don't like.