Glebe Primary School: Whole School Online Safety Policy

At Glebe Primary School we believe in an ethos that values the whole child. We strive to enable all children to achieve their full potential academically, socially and emotionally.

ICT skills and knowledge are vital to access life-long learning and employment. ICT is now seen as a functional, essential life-skill along with English and mathematics. The Internet is an essential element in 21st century life for education, business and social interaction. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology, including the Internet, and the 2014 computing curriculum aim states that pupils are 'responsible, competent, confident and creative users of information and communication technology.' According to the 2014 computing curriculum, across key stage 1 and 2, pupils should be taught how to use the Internet efficiently and safely, report any concerns and to develop a responsible and mature approach to accessing and interpreting information. The Internet can benefit the professional work of staff and enhances the school's management information and business administration systems. Ofsted guidance now states that "Online Safety training for staff must be integrated, aligned and considered as part of the overarching safeguarding approach."

Children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the Internet and other technologies. Some of the issues and risks are summarised below:

Copyright infringement

Copyright law applies on the Internet, but is ignored by many young people who download and swap music files, cut and paste homework assignments from others' work, or even purchase whole assignments from online cheat sites without realising the implications and consequences.

Obsessive use of the Internet and ICT

There is the potential for children and young people to become obsessed with the Internet and related technologies. Factors such as spending a significant amount of time online, excessive access to social networking sites, excessive use of gaming devises, deterioration of the quality of school work, diminished sleep time, or negative impacts upon family relationships, may all be indicators that the Internet is taking too high a priority in a young person's life.

Exposure to inappropriate materials

There is a risk that when using the Internet, email or chat services, young people may be exposed to inappropriate material. This may be material that is pornographic, hateful or violent in nature, encourages activities that are dangerous or illegal, or is just age-inappropriate or biased. One of the key benefits of the web is that it is open to all, but unfortunately this also means that those with extreme political, racist or sexist views have an unrestricted open communication channel.

In the case of pornography, there is no doubt that the Internet plays host to a large amount of legal and illegal material. Curiosity about pornography is a normal part of sexual development, but much of the material online is inappropriate for young people. It is not known what the long-term effects of exposure to such images may be.

Inappropriate or illegal behaviour

Young people may get involved in inappropriate, antisocial or illegal behaviour while using new technologies. Just as in the real world, groups or cliques can form online, and activities that start out as harmless fun, such as voicing an opposing opinion to another member of a chat room, can quickly escalate to something much more serious. This is evermore the case with the rise in popularity and use of social networking sites.

Online bullying is an unfortunate aspect of the use of new technologies, perceived as providing an anonymous method by which bullies can torment their victims at any time of day or night. While a young person may not be in physical danger, they may receive email, chat or text messages that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological well-being.

Some children and young people may become involved in much more serious activities. Possible risks include involvement in identity theft or participation in hate or cult websites, or the buying and selling of stolen goods. The ease of access to online gambling, suicide sites, sites for the sale of weapons, hacking sites, and sites providing recipes for drug or bomb making are also of great concern.

Young people may also become involved in the viewing, possession, making and distribution of indecent and/or child pornographic images. Any concern relating to criminally obscene or criminally racist content can be reported to the Internet Watch Foundation or the police.

Physical danger and sexual abuse

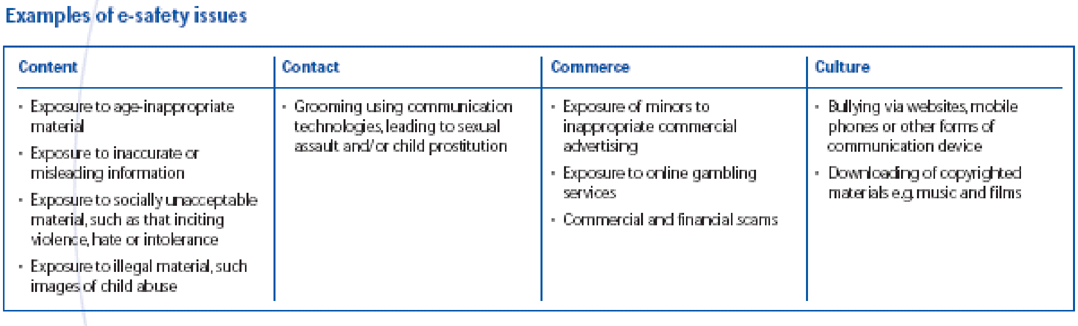
The threat of physical danger is perhaps the most worrying and extreme risk associated with the use of the Internet and other technologies.

A criminal minority make use of the internet and related services such as chat rooms to make contact with young people. The intention of these people is to establish and develop relationships with young people with the sole purpose of persuading them into sexual activity. Paedophiles will often target specific individuals, posing as a young person with similar interests and hobbies in order to establish an online ‘friendship’. These relationships may develop over days or weeks, or even months or years, as the paedophile gains the trust and confidence of the young person, perhaps progressing to other forms of contact such as text messaging as a prelude to meeting in person. These techniques are often known as ‘online enticement’, ‘grooming’ or ‘child procurement.’ The Sexual Offences Act 2003, which came into force in May 2004, includes a grooming offence specifically introduced to combat this abuse of the Internet and young people.

There is also a risk that while online a young person might provide information that can personally identify them or others, or arrange to meet people they have met online, so posing a risk to their safety or that of their family or friends.

Inappropriate or illegal behaviour by school staff

Unfortunately, school staff have also been found to have been involved in inappropriate or illegal behaviour relating to ICT use. This may include viewing or circulating inappropriate material via email, or much more serious activities such as viewing, possessing, making or distributing indecent and/or child pornographic images. Schools also have a responsibility, therefore, to educate staff as to acceptable behaviours online, and to monitor school networks for evidence of inappropriate activity. Inappropriate activity by a staff member may result in a disciplinary response by the school or authorities. If illegal behaviour by a staff member is suspected, the school has a duty to consult with the police at the earliest opportunity, preserving any potential evidence.



Examples of e-safety issues

Content	Contact	Commerce	Culture
• Exposure to age-inappropriate material • Exposure to inaccurate or misleading information • Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance • Exposure to illegal material, such images of child abuse	• Grooming using communication technologies, leading to sexual assault and/or child prostitution	• Exposure of minors to inappropriate commercial advertising • Exposure to online gambling services • Commercial and financial scams	• Bullying via websites, mobile phones or other forms of communication device • Downloading of copyrighted materials e.g. music and films

It is important to remember that whilst procedures and technologies are in place to ensure safe use of ICT within school, there will be issues outside of school that will be brought in. The school must be prepared to deal with these instances accordingly. They may impact on the child's well being and their relationships within school. In addition, this policy will address issues that may arise from the children using their own, increasingly sophisticated, range of handheld devices which may provide them with alternative access to potentially unsuitable materials.

We have a major responsibility to educate our pupils; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies.

Advice taken from:
E-Safety, Developing whole-school policies to support effective practice.
Becta ICT Advice 2005.

Aims of Glebe Primary School's Online safety policy

- to ensure that children and staff are working in a safe ICT learning environment
- to establish a clear understanding of the responsibilities of all those involved in the education of children at Glebe with regard to online safety, including the pupils (according to the 2014 curriculum), staff, governors and parents
- to educate all members of the school community to use the internet and digital technology in an effective and safe way both at school and home

Objectives:

Aim 1

• To ensure that an infrastructure of effective policies and procedures are in place and is the backbone of effective practice

• To ensure that an effective range of technological tools are in place to safeguard both pupils and the system itself:

- Firewall and virus protection
- Educational ISP – LGfL, monitored, high-speed, filtered content
- URL and E-mail filtering to minimise access to inappropriate content on the school system
- Wireless Network used in school is secure
- Devises taken off site are encrypted if they include sensitive data including pupil information

• To ensure there are clear policies and approval processes regarding the content that can be loaded to the school's website

• To ensure that the school adopts safe practices regarding the publication of images and names of pupils on the school website

• To ensure the website is regularly checked to make sure that there is no content that compromises the safety of pupils and staff (in place)

Aim 2

• To form an internet safety policy team led by the online safety co-ordinator to review and advise on online safety policies

- N.Reed (Online safety Co-ordinator)
- M. Penney (Head Teacher & Child Protection Officer)
- Paul Inspire (Network Technician)
- Steve Youens (link ICT Governor)
- School Council Representatives (pupils)

- To develop and implement a safety education programme for pupils, staff and the wider community. Staff development in online safety issues and how to respond to specific instances of misuse will be provided in school regularly. Key staff will also attend appropriate training when applicable throughout the year. Parents and the wider community will be informed of online safety policy and strategy either via an ICT Parents Evening and the school website.

Policy for acceptable use of E-Technologies by pupils

ICT can offer many positive educational and social benefits to young people, but unfortunately there are some dangers. Children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the Internet and other technologies. At Glebe, we value highly, the rich range of resources and experiences that the Internet and other technologies can offer to both our staff and pupils. The use of the Internet, web cams and e-mail is embedded into our schemes of work and enables us to teach and learn in ways that were previously unavailable.

Aims of this policy:

- to ensure that all pupils are working in a safe ICT learning environment, in school and at home, as laid out by the 2014 computing curriculum
- to establish a clear understanding of pupil responsibilities with regard to online safety both in school and at home, as laid out by the 2014 computing curriculum

Objectives (linked with the 2014 computing curriculum):

- to educate pupils in acceptable behaviours when using ICT, the Internet and other related technologies e.g. iPads, chat rooms, games consoles and e-mail both in school and at home
- to ensure all pupils are aware of procedures they should follow if they come across anything that is offensive or worrying
- to ensure all pupils are aware of sanctions that are in place if school policy is broken

Responsibilities:

Pupils must:

Respect all ICT equipment, hardware and software

Keep their usernames and passwords safe and secret and are not permitted to use anyone else's LGfL email account

Be aware of and follow the safe use of technology guidelines taught throughout the school.

Be aware of the sanctions that are in place if these guidelines are not followed.

Report any incidents of ICT misuse within the school to a member of the teaching staff.

Report any incidents of ICT misuse outside of school to a trusted adult.

Seek help or advice from a teacher, trusted adult or dedicated group e.g. Childline, CEOP if they experience problems when on line, or if they receive any content or contact which makes them feel uncomfortable in any way

Communicate with their parent(s)/carer(s) about online safety issues and follow school guidelines for the use of the Internet and other related technologies at home

Any accidental access to inappropriate or banned content must be reported to a member of school staff

Be aware of their social responsibilities with regard to using the Internet and other related technologies

Pupils must not:

Bring removable devises (eg a memory stick) in to school

E-mail malicious attachments into school or to others.

Bring any form of handheld device into school e.g. mobile phones, handheld computers, I Pods or games consoles.

Try to access chat rooms or instant messaging systems when in school

Send any kind of malicious message, image or web link.

Try to access inappropriate material of any sort (including pornographic, racial hatred, religious hatred or any material not related to the lesson).

Pass on the account usernames and passwords of others to a second party

Attempt to contact members of staff through social networking sites

Procedure:

If a child is found to misuse any piece of ICT equipment then their class teacher is to impose appropriate sanction e.g. damage, parents to be informed, issue discussed. Offence is to be logged with the online safety co-ordinator and DHT responsible for behaviour.

If a child is found to be copying information for their assignments and failing to acknowledge the source of information (plagiarism and copyright infringement) then the issue will be discussed with the child with their class teacher.

If a child is found to be trying to access inappropriate material (pornographic sites, racial hatred or religious hatred, sexist jokes, drug or bomb making recipes, chat rooms, instant messaging services) then their class teacher, head teacher and parents to be informed, issue discussed. Procedures outlined in bullying policy for racial or religious abuse to be followed. Offence is to be logged via e-mail to the online safety co-ordinator and outside agencies alerted if deemed appropriate by the head teacher.

If a child is found to be sending offensive or malicious messages via e-mail or other communication technologies then the online safety co-ordinator is to be informed who will consult with the borough (to identify the message) and the head teacher. Sanctions appropriate to the offence will be discussed and implemented. Offence to be logged.

If a child is found to be malicious attachments via e-mail or other communication technologies then the online safety co-ordinator is to be informed who will consult with the borough (to identify the message) and the head teacher. Sanctions appropriate to the offence will be discussed and implemented. Offence to be logged.

If a pupil is found to be using other usernames and passwords other than their own for any reason then the online safety co-ordinator is to be informed who will consult with the borough (to identify when the account was accessed and from where) and the head teacher. Sanctions appropriate to the offence will be discussed and implemented. Offence to be logged.

If a pupil passes on the account usernames and passwords of others to a second party then the online safety co-ordinator and the head teacher are to be informed. Sanctions appropriate to the offence will be discussed and implemented. Offence to be logged.

If a pupil approaches a member of staff after receiving content or contact which makes them feel uncomfortable in any way then that member of staff is to report the incident to the online safety co-ordinator who will consult with the head teacher. Offence to be logged. The child protection officer will be involved if the incident could compromise the well being of a child.

If accidental access to inappropriate or banned content is reported then the online safety co-ordinator must be informed with URL, time, date and person who accessed site. URL will be passed onto the borough for blocking and the Head Teacher informed. The incident will be logged and parents informed if deemed necessary.

Any instances of potentially illegal behaviour using the technologies at hand e.g. viewing, possession, making and distributing indecent images of children and serious stalking or harassment facilitated by communication technologies must be reported to the online safety co-ordinator and Head Teacher immediately. The computer(s) is to be left switched on and no-one is to use it. It may be necessary to shut down the entire network. The police must be informed and head teacher is to seek legal advice via the LA, as soon as possible.

Any messages of bullying related to Racial Hatred or Religious Hatred to be reported to the online safety co-ordinator and Head Teacher and the police informed if deemed necessary. Legal advice to be taken from the borough, parents consulted and incident logged. Appropriate sanctions implemented. Counselling may need to be offered to both victim(s) and perpetrator(s).

Pen drives, and any other removable media will be confiscated and handed back to Parent(s)/Guardian(s). If a piece of homework is brought in on such a device then an appropriate member of staff must check any files on the device using an up to date virus checker.

The online safety co-ordinator will monitor incidents and will react pro-actively to any emerging behaviours or issues.

Glebe Primary School pupil code of conduct for the use of technology:

ICT can offer many positive educational and social benefits to young people, but unfortunately there are some dangers. Children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. At Glebe, we value highly, the rich range of resources and experiences that the Internet and other technologies can offer to both our staff and pupils. The use of the Internet, web cams and e-mail is embedded into our schemes of work and enables us to teach and learn in ways that were previously unavailable.

As a pupil of Glebe Primary School, you must:

- Respect all ICT equipment (computers, cameras, iPads etc)
- Follow school rules on ICT and online safety
- Be aware of the sanctions that are in place if these rules are not followed.
- Treat others with respect when using the Internet or other related technologies
- Keep your usernames and passwords safe and secret and you are not permitted to use anyone else's LGfL username and password for any reason.
- When possible, use appropriate search engines when searching for material: e.g. www.swiggle.org.uk
- Report any incidents of ICT misuse within the school to a member of the teaching staff.
- Report any accidental access to inappropriate or banned content must be reported to a member of school staff
- Report any incidents of ICT misuse outside of school to a trusted adult.
- Seek help or advice from a teacher or trusted adult if you experience problem when on line, or if you receive any content or contact which makes you feel uncomfortable in any way

As a pupil of Glebe Primary School, you must not:

- Bring removable devises eg pen drives into school
- Bring any form of handheld device in school e.g. mobile phones, handheld computers, other removable media, i-Pods or games consoles
- Knowingly e-mail malicious attachments into school or to others
- Send any kind of malicious message, image or web link
- Try to access inappropriate material of any sort
- Try to access chat rooms or instant messaging systems when in school
  Try to contact any member of staff via social networking sites eg Facebook

Any offences relating to the use of the Internet and related technologies will be dealt with by school staff, parents or guardians may be informed and appropriate sanctions imposed.

Pupils to sign an agreement form (see appendix 3)

Policy for acceptable use of E-Technologies by Staff

ICT and related technologies in Glebe Primary School are embedded within the work culture. Staff use ICT, the Internet, e-mail, iPads and other applications on a daily basis to maximise efficiency. We aim to continue developing the use of ICT in all working practices of staff at Glebe but we need to be aware of relevant issues when using such technology.

Aims of this policy:

- To ensure that all staff are working in a safe ICT learning environment
- To establish a clear understanding of staff responsibilities with regard to online safety

Objectives:

- To educate staff in acceptable behaviours when using ICT, the Internet and other related technologies when in school and at home. Staff development in online safety issues and how to respond to specific instances of misuse will be provided in school. Key staff will also attend borough led courses when applicable and will feed back on any relevant developments.

- To ensure all staff are aware of procedures they should follow if they come across anything that is offensive or worrying. Staff development in online safety issues and how to respond to specific instances of misuse will be provided in school. Key staff will also attend borough led courses when applicable and will feed back on any relevant developments.

- To ensure all staff are aware of sanctions that are in place if school policy is broken. Staff development in online safety issues and how to respond to specific instances of misuse will be provided in school. Key staff will also attend borough led courses when applicable and will feed back on any relevant developments.

Responsibilities:

Staff must be aware of all policy and procedure linked to online safety both in and out of the school.

Mobile phones must not be used to record images or video of pupils (e.g. on school trips). Parents on trips can use mobile phones or camera to take images (still or moving) of their children as long as the relevant consent forms are signed.

School cameras and iPads may be used to record images and video of pupils but these must be downloaded onto the school system and removed from the camera at the end of the day (iPads too). Staff have right to access for educational purposes only.

Downloading of material, within school, from the Internet is acceptable if the content is for educational purposes.

Staff have individual responsibilities to protect the security and confidentiality of the school network. Any confidential documents must be saved to an encrypted memory stick. Passwords must not be shared and staff must log off the teacher desktop when they leave a machine unattended. The password for teacher should be changed regularly.

The Internet and e-mail may be used in school for educational purposes. It may also be used for personal purposes as long as the content being viewed or sent is appropriate and is in line with professional standards.

The Internet and related technologies are not to be used for any form of illegal activity, for example downloading copyright materials, introducing viruses, sustained stalking via communication technologies or accessing banned content.

The use of the Internet and e-mail is monitored by the borough, e-mail and URL filtering systems, firewalls and anti virus protection is in place and covers the one feed from the LGfL to the WWW.

Accidental access to inappropriate or banned content must be reported to the online safety co-ordinator who will then provide the borough with the URL to be blocked

Staff must take measures to protect the system against viruses. They must have up to date anti-virus software on their laptops and must use a virus checker when using removable media e.g. USB Pen Drives or CD-ROMs.

School laptops, iPads and other devices must not be used for any illegal or inappropriate activities e.g. access to, or sharing of banned content.
(See appendix 4)

Staff must be aware of the importance of high privacy settings on social networking sites i.e. facebook and not contact pupils through non-school based social networking sites.

<u>Procedure:</u>

Reported incidents of misuse will be reported to the Head Teacher, online safety co-ordinator and appropriate staff at the LA. Outside agencies, including the police and counselling services, will be informed if deemed appropriate. All incidents will be logged. Legal advice will be obtained in cases of suspected illegal activity.

Any evidence of illegal behaviour on a school computer, laptop or other related technology will result in the isolation of the machine and maybe the freezing of the network. The police will be informed and the head teacher is to seek legal advice from the borough as soon as possible.

URL of inappropriate or banned content must be passed to the borough for blocking.

Accidental access to inappropriate or banned content must be passed to the borough for blocking.
(See appendix 5)

Social media policy

Staff and children are reminded through training and through teaching the importance of staying safe using social media. Strict privacy settings are advised, particularly for staff, to ensure they are not vulnerable at any time. Children are reminded that they should be extremely careful also, and social media such as Facebook isn't suitable for children under 13. Staff need to ensure they do not have any contact with children through social media

Policy for the use of e-mail in school

E-mail is an ever expanding part of culture at the school. Every child and staff member has an LGfL e-mail account. Staff are encouraged to share information through use of e-mail and it provides pupils with learning experiences that conventionally, would not be possible. We aim to continue developing the role of e-mail within the school but we need to be aware of harmful behaviours and how to deal with them (such as misuse of others' accounts, bullying, viruses, spamming and malicious attachments.)
Aim:

- To ensure that both pupils and staff are aware of safe and responsible behaviours when using e-mail

Objectives:

- To develop a whole school awareness of safe and responsible behaviours when using e-mail (including parents). Pupils will be taught safe and responsible behaviours when using e-mail and how to deal with any instances that worry them at relevant times throughout the school. Opportunities for the teaching of safe e-mail use will be begun in Year 3 and revisited whenever appropriate throughout the rest of the school. Parents and the wider community will be informed of e-mail policy and strategy.

- To ensure that technological tools to safe guard against malicious use of e-mail are in place, are working (in place) and that stakeholders know how to use them where appropriate e.g. to check attachments for viruses

- To develop a whole school awareness of the sanctions that will be applied if e-mail use is abused (including pupils and parents). Sanctions will relate to the seriousness of the misuse

- To incorporate the teaching of appropriate e-mail behaviour through teaching (including how to use e-mail appropriately out of school)

- To encourage pupils to use their LGfL e-mail accounts as oppose to other accounts as this system is secure and monitored.

Responsibilities:

Local Authority:

To install and maintain e-mail filtering and monitoring software
To install anti-virus software and keep it up to date
To provide e-mail addresses, usernames and passwords for all staff and pupils. Pupil usernames are random, preventing people working out which account belongs to whom.

To be aware of the risks pupils face when using e-mail.
To know the correct procedure to follow if a pupil informs them of any misuse of e-mail.
To be aware of and teach responsible behaviours when using e-mail where detailed in planning.
To keep their account username and password safe and not to use the usernames and passwords of others for any reason
To not send malicious, bullying or inappropriate material of any kind in any form - image, text, video, web link or attachment

LA Policy link -
https://static.lgfl.net/LgflNet/downloads/policies/LGfL%20Acceptable%20Use%20Policy.pdf
Procedures:

E-mail is to be used as a means of communication between parent(s)/carer(s) and for pupils to e-mail homework projects into school (with prior agreement). The school is able to send out emails to all parents via Parent Mail. This enables the school to keep parents informed in an efficient way.

If a child is found to be sending offensive or malicious messages via e-mail then the online safety co-ordinator is to be informed who will consult with the borough (to identify the message) and the head teacher. Sanctions appropriate to the offence will be discussed and implemented. Offence to be logged.

If a pupil is found to be using other usernames and passwords other than their own for any reason then the online safety co-ordinator is to be informed who will consult with the borough (to identify when the account was accessed and from where) and the head teacher. Sanctions appropriate to the offence will be discussed and implemented. Offence to be logged.

If a pupil approaches a member of staff after receiving content or contact which makes them feel uncomfortable in any way then that member of staff is to report the incident to the online safety co-ordinator who will consult with the head teacher. Offence to be logged. The child protection officer will be involved if the incident could compromise the well being of a child.

Any instances of potentially illegal behaviour using the technologies at hand e.g. viewing, possession, making and distributing indecent images of children and serious stalking or harassment facilitated by communication technologies must be reported to the online safety co-ordinator and Head Teacher immediately. The computer(s) is to be left switched on and no one is to use it. It may be necessary to shut down the entire network. The police must be informed and head teacher is to seek legal advice via the LA, as soon as possible.

The online safety team will review infringements and make amendments to policy as appropriate. The online safety co-ordinator will monitor incidents and will react pro-actively to any emerging behaviours or issues.

Policy for the teaching of Online safety

We have a legal responsibility to educate our pupils on internet safety, as laid out by the 2014 computing curriculum; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

Aim:

- To teach both pupils and staff the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies
- To train staff to be able to respond appropriately and follow procedures when dealing with issues arising from pupils' use of the Internet and related technologies.

Objectives:

- To explicitly teach children internet safety and their roles of being responsible digital users, according to the 2014 computing curriculum.

- To teach all pupils, using associated activities, the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies

- To identify training opportunities for staff that will enable them to become more familiar with the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies and when dealing with online safety issues arising from pupils' experiences. Staff development in online safety issues and how to respond to specific instances of misuse will be provided in school. Key staff will also attend LA led courses when applicable.

Actions:

The teaching of online safety should be an integral of the computing teaching provision in all year groups. It should be age and experience appropriate. The computing subject leader should ensure it is being taught according to the curriculum requirements and combine with the PSHE subject leader to identify opportunities in all other relevant schemes of work. Online safety should be given a high profile in school both through lesson planning and the wider curriculum eg designated assemblies, display boards, focus days etc.

School Website Policy

At Glebe we aim to develop a website which is effective and does not compromise the safety of pupils or staff. It will provide details of the school, show examples of children's work, give useful links including OfSTED reports and latest news bulletins. It will be kept up to date and relevant to school issues.

Aim:

To ensure that the school website is effective and does not compromise the safety of pupils and staff.

Objectives:

To have a system in place for monitoring and updating the website

To follow policy and approved procedures (below) regarding the content that can be uploaded to the site

To adopt safe practices regarding the publication of images and names of pupils on the site

To ensure that the school is not infringing the intellectual property rights of others through any of the materials via the site (copyright may apply to text, images, music or video that originate from other sources)

To protect the school's own copyright in terms of its material published on the web. Investigate actions needed to put this into place.

Responsibilities and procedures:

Access to the website via password is restricted to the Computing co-ordinator, Head Teacher and administrative staff (Karen Hampshire and Joanna Crawford) who are trained for the uploading and maintaining of current information.

The online safety co-ordinator or HT will approve the content to be uploaded to the website and will monitor what is on the site on a weekly basis. Any content deemed inappropriate will be removed and its source investigated. Normally the site is updated on a Friday afternoon and subsequently cross checked.

The copyright of any content uploaded to the site is checked and if necessary, indicated on the site. The school's own copyright in terms of its material published on the web site is clearly indicated.

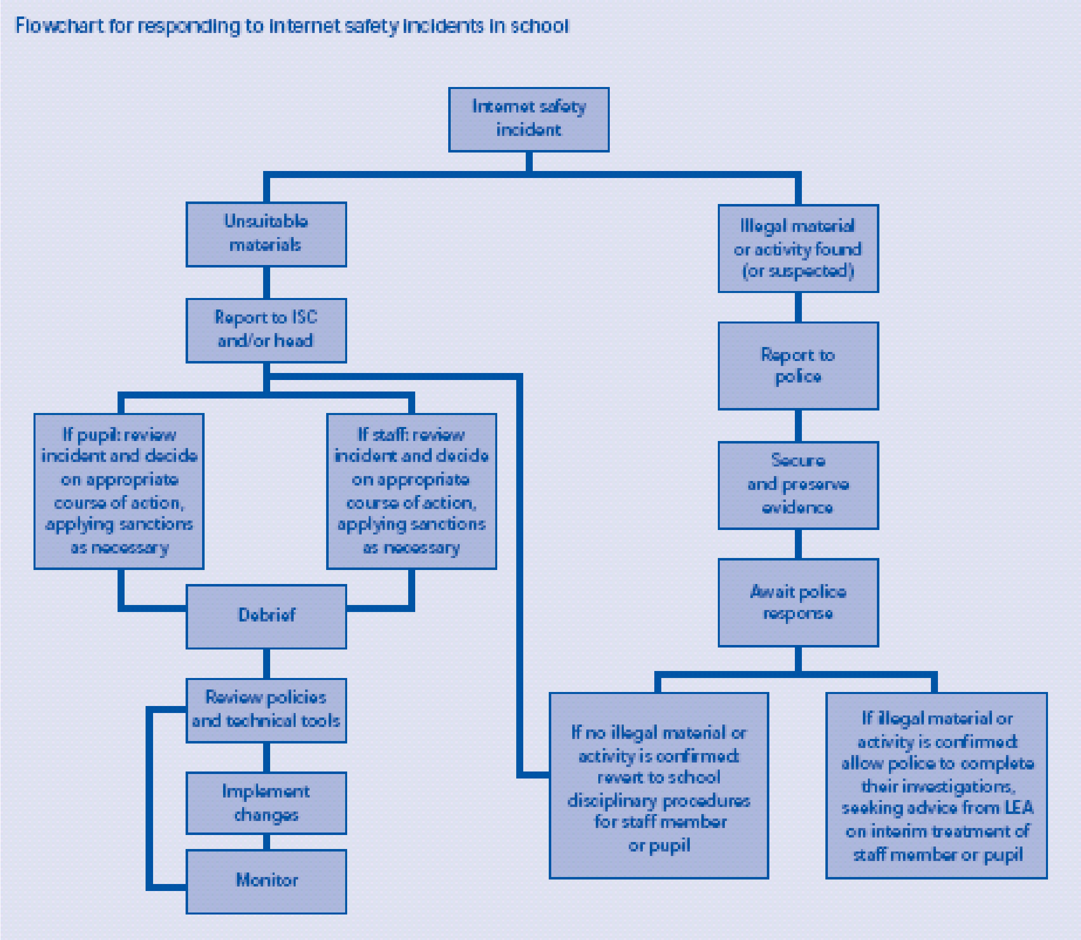
Parental permission must always be obtained before any image of a pupil is uploaded to the web site (generic consent forms sent out to every family). First name and last name are not to appear with the photo. If a child's image is not used, their name may be, if appropriate e.g. with a piece of work with parental permission. The image file name is not to contain any reference to the child – name, class, age or any form of tag. All images are stored on password protected desktop on the schools server. Only images of pupils in appropriate dress will be used to minimise the chance of inappropriate use.

If any reports of images being used inappropriately reach the school, the Head Teacher, online safety co-ordinator and Child Protection Officer will be informed if deemed necessary. Legal advice will be sought from the borough if deemed necessary and the police will be informed.

Advice taken from:

E-Safety, Developing whole-school policies to support effective practice. Becta ICT Advice 2005.

Appendix 1


Flowchart for responding to internet safety incidents in school

Internet safety incident
Unsuitable materials
Illegal material or activity found (or suspected)
Report to ISC and/or head
Report to police
If pupil: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Secure and preserve evidence
Await police response
Debrief
Review policies and technical tools
Implement changes
Monitor
If no illegal material or activity is confirmed revert to school disciplinary procedures for staff member or pupil
If illegal material or activity is confirmed allow police to complete their investigations, seeking advice from LEA on interim treatment of staff member or pupil

ISC = Online safety Co-ordinator
Appendix 2

Pupil sanctions for misuse of the internet and other related technologies

Misuse	Procedure	Sanction
ICT equipment not treated with respect e.g. damage or deletion of school's or others' files and apps	Class teacher is to impose appropriate sanction and discuss issue with child; parents to be informed, Offence is to be logged with the online safety co-ordinator.	Parents informed, repeat misuse will lead to invoicing for replacement

Deliberate access to another person's e-mail account.	If a pupil is found to be using other usernames and passwords other than their own for any reason then the online safety co-ordinator is to be informed who will consult with the borough (to identify when the account was accessed and from where) and the head teacher. Sanctions appropriate to the offence will be discussed and implemented. Offence to be logged.	Parents informed. Warning. Re-occurrence will lead to a two week 'freezing' of the perpetrators accounts. Further re-occurrence could lead to permanent 'freezing' of perpetrators' accounts and he/she will have no unsupervised access to school ICT equipment.
Passing on the account usernames and passwords of others to a third party	If a pupil passes on the account usernames and passwords of others to a third party then the online safety co-ordinator and the head teacher are to be informed. Offence to be logged.	Parents informed. Warning. Re-occurrence will lead to a two week 'freezing' of the perpetrators accounts. Further re-occurrence could lead to permanent 'freezing' of perpetrators accounts and he/she will have no unsupervised access to school ICT equipment.
Trying to access chat rooms or Instant Messaging Services	If a pupil tries to access chat rooms or Instant Messaging Services then the Online safety Co-ordinator and the head teacher are to be informed. Offence to be logged.	Repeat misuse will lead to parents informed and perpetrator having no unsupervised access to school ICT equipment.

Sending malicious messages using ICT.	If a child is found to be sending malicious messages via email or other communication technologies then the online safety co-ordinator is to be informed who will consult with the borough (to identify the message) and the head teacher. Sanctions appropriate to the offence will be discussed and implemented. Offence to be logged.	Parents informed. Two week 'freezing' of the perpetrators accounts. Further re-occurrence could lead to permanent 'freezing' of accounts and no unsupervised access to school ICT equipment. Sanctions that follow guidelines in Anti-Bullying Policy.
Plagiarism or copyright infringements	If a child is found to be copying information for their assignments and failing to acknowledge the source of information then the issue will be discussed with the child with their class teacher and the online safety co-ordinator and Head Teacher if there are successive instances of infringement. Offence to be logged	Parents informed and work will not be marked. Warning. Repeat misuse will lead to perpetrator having no unsupervised access to school ICT equipment.
Knowingly sending malicious e-mail attachments	If a child is found to be malicious attachments via e-mail or other communication technologies then the online safety co-ordinator is to be informed who will consult with the borough (to identify the message) and the head teacher. Offence to be logged.	Parents informed. Two week 'freezing' of the perpetrators accounts. Further re-occurrence could lead to permanent 'freezing' of accounts and no unsupervised access to school ICT equipment. Sanctions that follow guidelines in Anti-Bullying Policy.
Bringing mobile phones or other prohibited handheld devices into school	Confiscation, inform parents. Hand back to parents. Offence to be logged.	Parents informed, repeat misuse will lead to sanctions in accordance with the school behaviour policy.

Deliberately trying to access inappropriate or banned content	If a child is found to be trying to deliberately access inappropriate material (pornographic sites, racial hatred or religious hatred, sexist jokes, drug or bomb making recipes) then their class teacher, head teacher and parents to be informed, issue discussed. Procedures outlined in bullying policy for racial or religious abuse to be followed. Offence is to be logged via e-mail to the online safety co-ordinator and outside agencies alerted if deemed appropriate by the head teacher.	Parents informed. Warning. No unsupervised access to school ICT equipment. Possible suspension for repeat offence.
Sending messages via communication technology relating to racial of religious hatred	Any messages of bullying related to Racial Hatred or Religious Hatred to be reported to the online safety co-ordinator and Head Teacher and the police informed if deemed necessary. Legal advice to be taken from the borough, parents consulted and incident logged. Appropriate sanctions implemented. Counselling may need to be offered to both victim(s) and perpetrator(s).	Parents informed. Warning. No unsupervised access to school ICT equipment. Possible suspension for repeat offence.
Using communication technology for the purpose of bullying others.	Follow guidelines in Anti-Bullying Policy	Parents informed. No unsupervised access to school ICT equipment. Follow guidelines in Anti-Bullying Policy

Appendix 3 – Pupil online safety agreement form

Glebe Primary School Online safety agreement form

Name:

As a pupil of Glebe Primary School, I will:

- Respect all ICT equipment (computers, cameras, iPads etc)
- Follow school rules on ICT and online safety
- Be aware of the sanctions that are in place if these rules are not followed.
- Treat others with respect when using the Internet or other related technologies
- Keep your usernames and passwords safe and secret and you are not permitted to use anyone else's LGfL username and password for any reason.
- When possible, use appropriate search engines when searching for material: e.g. Google

- Report any incidents of ICT misuse within the school to a member of the teaching staff.
- Report any accidental access to inappropriate or banned content must be reported to a member of school staff
- Report any incidents of ICT misuse outside of school to a trusted adult.
- Seek help or advice from my teacher or trusted adult if you experience problem when on line, or if you receive any content or contact which makes you feel uncomfortable in any way.

As a pupil of Glebe Primary School, I will not:

- Bring removable devises eg pen drives into school
- Bring any form of handheld device in school e.g. mobile phones, handheld computers, other removable media, i-Pods or games consoles
- Knowingly e-mail malicious attachments into school or to others
- Send any kind of malicious message, image or web link
- Try to access inappropriate material of any sort
- Try to access chat rooms or instant messaging systems when in school

Furthermore I will not try to contact any member of staff via social networking sites eg Facebook.
I know that Mr Reed is the teacher responsible for online safety at Glebe.

I know that any offences relating to the use of the Internet and related technologies will be dealt with by my school staff and my parents or guardians may be informed and appropriate sanctions imposed.

Signed: ________________________________ Date: _______________

Appendix 4 – Staff acceptable use policy

	Name of School	**Glebe Primary**
	AUP review Date	**July 2017**
	Date of next Review	**July 2019**
	Who reviewed this AUP?	**MP and AS**

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school’s digital technology resources and systems for Professional purposes or for uses deemed ‘reasonable’ by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow ‘good practice’ advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else’s password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school’s network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.
(This is currently: hillingdongrid.org)
- I will only use the approved school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact (Nicholas Reed).
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep

any ‘loaned’ equipment up-to-date, using the school’s recommended anti-virus, firewall and other ICT ‘defence’ systems.

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home or on personal devises.
- I will use the school’s Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer, laptop or iPad loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any “significant personal use” as defined by HM Revenue & Customs.
- I will access school resources remotely (such as from home) only through the LGfL / school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school’s information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school’s online safety curriculum into my teaching.
- I will alert the school’s named child protection officer / relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): Staff agreement form

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature .... Date ....

Full Name .... (printed)

Job title ....

School ....

Authorised Signature (Head Teacher (primary) / Head/Deputy/ senior teacher (secondary)

I approve this user to be set-up.

Signature .... Date ....

Full Name: Melanie Penney (HT)

Appendix 5 – Reporting online safety concerns (guidance)

	Name of School	**Glebe Primary**
	Guidance review Date	**July 2017**
	Date of next Review	**July 2019**
	Who reviewed this guidance?	**MP and AS**

Guidance: What do we do if?

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered (LGfL schools report to: **webalerts@synetrix.com**).
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed intentionally by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA/RBC.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
   - Remove the PC to a secure place.
   - Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (contact Personnel/Human Resources).
   - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local police or High Tech Crime Unit and follow their advice.
   - If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including online safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.

5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform the LA online safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA online safety officer.

The school may wish to consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA online safety officer.
6. Consider delivering a parent workshop for the school .community.

All of the above incidences must be reported immediately to the head teacher and online safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

This policy was reviewed and updated in July 2017 by Alice Smith (computing coordinator)

Next policy review in July 2019 (or sooner if necessary)