GOLDFINCH PRIMARY
Building Excellence

e-Safety Policy (Draft)

Spring 2018

Next Review Date: Spring 2019

Signed: Chair of Governors ……

Head Teacher ……

Introduction

This policy applies to all members of the our school community (including staff, students / pupils, volunteers, parents / carers and visitors) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

At Goldfinch we will deal with such incidents within this policy and associated Behaviour and Anti-Bullying Policies and will, where known, inform parents / carers of incidents of inappropriate e-Safety behaviour that take place out of school.

e-Safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Our e-Safety policy will operate in conjunction with other policies including ICT, Anti-Bullying, Safeguarding/Child Protection, Data Protection and Behaviour. Our e-Safety policy is based on Wandsworth Children's Services e-Safety Policy and government guidance. It is split into three main sections:-

- Teaching and Learning
- Managing internet access
- Communications Policy

The e-Safety policy and its implementation will be reviewed annually and there are two named e-Safety co-ordinators within Goldfinch – **Emilie Haston and Robert Slezak.**

End to End e-Safety

e-Safety depends on effective practice at a number of levels:-

- Responsible ICT use by all staff and students, encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering systems.

Staff training

It is essential that all staff receive e-Safety training and understand their responsibilities, as outlined in this policy.

A planned programme of formal e-safety training will be made available to staff and it is expected that some staff will identify e-Safety as a training need within the performance management process. All new staff should receive e-Safety training as part of their induction programme,

ensuring that they fully understand the school e-Safety policy and acceptable use policies which are signed as part of their induction.

The e-Safety Leader will receive regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority and others. All teaching staff are asked to sign a checklist stating they have read and understood this e-Safety policy and are therefore aware of its content. The e-Safety Leader will provide advice, guidance and training as required to individuals as required on an on-going basis.

Teaching and Learning

Why is internet use important?

- The internet is an essential element in 21st Century life for education and social interaction. Goldfinch Primary School has a duty to provide children with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and children.

Enhancing learning through the internet

- Internet access will be designed expressively for pupil use and will include filtering appropriate to the age of the pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Evaluating internet content

- We will ensure that the use of the internet derived materials by staff and children complies with copyright law.
- Children should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children will be taught how to be aware of internet safety and risks involved with social network sites, contacting strangers and cyber-bullying.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Pupil use of the internet must be supervised at all times. If a child should come across any website or message which is inappropriate, they should switch off the monitor and alert an adult. The adult should then note the website and report using the ICT Fault Log book. The website can be investigated further and reported to Wandsworth IT to be blocked.

Information System Security

- ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Wandsworth Children's Services ICT support.

Email

- Pupils may only use approved email accounts on the school system (these will only be released when the class is working on emails within their topic. They will then be suspended once the topic is complete).
- Pupils must immediately tell a member of staff if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on our website are the school address, email and telephone number. Staff or children's personal information will not be published.
- The Headteacher will take overall responsibility and ensure that content is accurate and appropriate.

Publishing children's images and work.

- Photographs that include children will be selected carefully and will not enable individual children to be identified.
- Children's full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

Managing filtering

- The school will work with the LA, DCSF and the internet service provider to ensure systems to protect children are reviewed and as effective as possible.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Leader. ULR, time and date should be recorded.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing

- Pupils require permission from a supervising member of staff before making or supervising a video conference call.

Managing emerging technologies

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

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

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

Policy Decisions

Authorising internet access

- All staff, including Teaching Assistants and Supply Teachers must read and sign the acceptable ICT Acceptable User Policy (AUP) before using any school ICT resource.
- In the EYFS and Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Pupils will be asked to sign and return an Acceptable Use Agreement form (see Appendix)

Assessing risks

- We will take all reasonable precautions to ensure that all users access only appropriate material. However, due to the international scale and linked nature of the internet content, it is not possible to guarantee that unsuitable material will never appear on a computer.
- Neither Goldfinch Primary School nor Wandsworth Council can accept liability for the material accessed or any consequence of internet access.
- We will audit ICT provision to establish if the e-Safety Policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature will be dealt with in accordance with the procedures in our Safeguarding/Child Protection Policy.
- Children and parents will be informed of the complaints procedure.

Community use of the internet

- We will be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- Parents using school ICT equipment must sign an AUP consent form prior to use (e.g. parent workshops for Numeracy and Literacy).

Communications Policy

Introducing the e-Safety Policy to children

- The policy will be shared with pupils at the beginning of every term.
- e-Safety rules will be displayed in classrooms and discussed with children through out the year (see Appendix).
- Pupils will be informed that network and internet use will be monitored.

Staff and the e-Safety Policy

- All staff will be given a copy of the e-Safety policy and its importance explained.

- Staff are made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents/ Carers will be drawn to the e-Safety Policy at the Curriculum Evening, in newsletters, workshops and our school website.

Illegal or Inappropriate Activities and Related Sanctions

The school believes that the activities listed below are inappropriate in a school context (those in bold are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images **(illegal - The Protection of Children Act 1978)**
- grooming, incitement, arrangement or facilitation of sexual acts against children **(illegal – Sexual Offences Act 2003)**
- possession of extreme pornographic images **(illegal – Criminal Justice and Immigration Act 2008)**
- criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) **(illegal – Public Order Act 1986)**
- pornography
- sexting
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally the following activities are also considered unacceptable on ICT kit provided by the school:

- using school systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Wandsworth Council and / or the school
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- on-line gambling and non-educational gaming
- use of personal social networking sites / profiles for non-educational purposes.

Youth produced sexual imagery (sexting) [1]

[1] Youth refers to all people under the age of 18.

The practice of children sharing images and videos via text message, email, social media or mobile messaging apps has become commonplace. However, this online technology has also given children the opportunity to produce and distribute sexual imagery in the form of photos and videos. Such imagery involving anyone under the age of 18 is illegal.

Youth produced sexual imagery refers to both images and videos where;

- A person under the age of 18 creates and shares sexual imagery of themselves with a peer under the age of 18.
- A person under the age of 18 shares sexual imagery created by another person under the age of 18 with a peer under the age of 18 or an adult.
- A person under the age of 18 is in possession of sexual imagery created by another person under the age of 18.

All incidents of this nature should be treated as a safeguarding concern and in line with the UKCCIS guidance 'Sexting in schools and colleges: responding to incidents and safeguarding young people'[2].

- Cases where sexual imagery of people under 18 has been shared by adults and where sexual imagery of a person of any age has been shared by an adult to a child is child sexual abuse and should be responded to accordingly.
- If a member of staff becomes aware of an incident involving youth produced sexual imagery they should follow the child protection procedures and refer to the DSL as soon as possible.
- The member of staff should confiscate the device involved and set it to flight mode or, if this is not possible, turn it off. Staff should not view, copy or print the youth produced sexual imagery.
- The DSL should hold an initial review meeting with appropriate school staff and subsequent interviews with the children involved (if appropriate). Parents should be informed at an early stage and involved in the process unless there is reason to believe that involving parents would put the child at risk of harm. At any point in the process if there is concern a young person has been harmed or is at risk of harm a referral should be made to Children's Social Care or the Police as appropriate.
- Immediate referral at the initial review stage should be made to Children's Social Care/Police if;

1. The incident involves an adult;
2. There is good reason to believe that a young person has been coerced, blackmailed or groomed or if there are concerns about their capacity to consent (for example, owing to special education needs);
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the child's development stage or are violent;
4. The imagery involves sexual acts;
5. The imagery involves anyone aged 12 or under;
6. There is reason to believe a child is at immediate risk of harm owing to the sharing of the imagery, for example the child is presenting as suicidal or self-harming.
7. If none of the above apply then the DSL will use their professional judgement to assess the risk to pupils involved and may decide, with input from the Headteacher, to respond to the incident without escalation to Children's Social Care or the police.

In applying judgement the DSL will consider if;

---

2 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

- there is a significant age difference between the sender/receiver;
- there is any coercion or encouragement beyond the sender/receiver;
- the imagery was shared and received with the knowledge of the child in the imagery;
- the child is more vulnerable than usual i.e. at risk;
- there is a significant impact on the children involved;
- the image is of a severe or extreme nature;
- the child involved understands consent;
- the situation is isolated or if the image been more widely distributed;
- there other circumstances relating to either the sender or recipient that may add cause for concern i.e. difficult home circumstances;
- the children have been involved in incidents relating to youth produced imagery before.

If any of these circumstances are present the situation will be escalated according to our child protection procedures, including reporting to the police or children's social care. Otherwise, the situation will be managed within the school.

The DSL will record all incidents of youth produced sexual imagery, including both the actions taken, actions not taken, reasons for doing so and the resolution in line with safeguarding recording procedures.

Sanctions

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupil sanctions	Refer to class teacher	Refer to e-safety coordinator	Refer to head teacher	Refer to Police	Refer to e-safety coordinator for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓		✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓				✓		✓		
Unauthorised use of mobile phone / digital camera / other handheld device	✓		✓			✓			
Unauthorised use of social networking / instant messaging / personal email	✓				✓				
Unauthorised downloading or uploading of files	✓				✓				
Allowing others to access school network by sharing username and passwords	✓	✓	✓		✓		✓		

Attempting to access the school network, using another pupil's account	✓	✓	✓		✓		✓		
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓	✓				✓		
Corrupting or destroying the data of other users	✓	✓	✓			✓	✓	✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓		✓	
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓		✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓			✓		✓	
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓		✓		✓	✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓	✓			
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓		✓	✓	✓	✓	

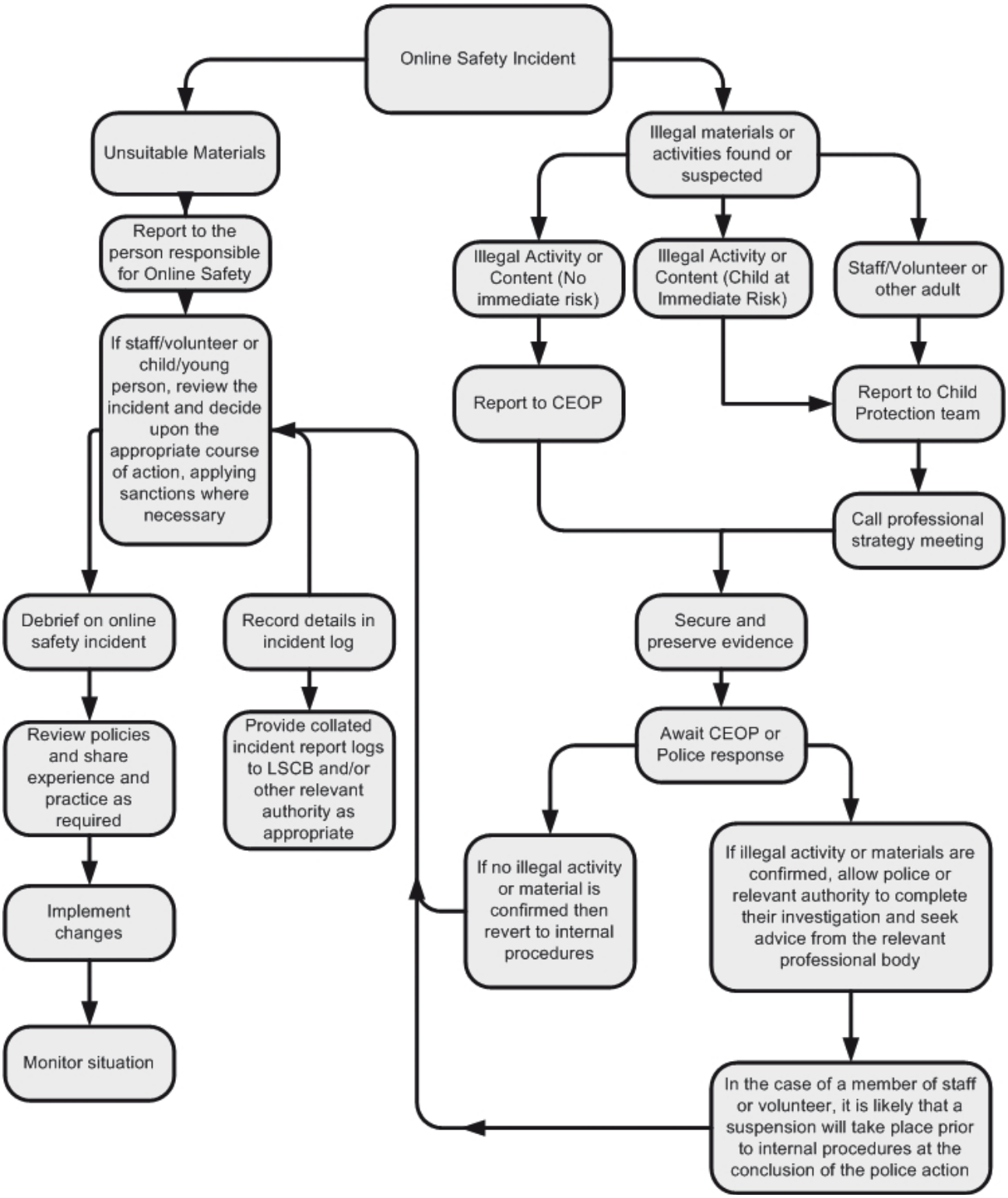
Staff sanctions

	Refer to line manager	Refer to head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓	✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓			✓	✓		
Unauthorised downloading or uploading of files	✓	✓			✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓				✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓	✓				✓		
Deliberate actions to breach data protection or network security rules	✓	✓			✓	✓	✓	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓			✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓	✓	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	✓	✓	✓			✓		
Actions which could compromise the staff member's professional standing	✓	✓				✓		

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓				✓		
Using proxy sites or other means to subvert the school's filtering system	✓	✓			✓	✓	✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓			✓	✓		
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓		✓	✓	✓	
Breaching copyright or licensing regulations	✓	✓				✓		
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓			✓	✓	✓

Reporting of e-Safety breaches

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:-



Monitoring of this policy

This policy will be reviewed annually by the Senior Leadership Team and e-Safety Leader, giving consideration to:

- The latest Ofsted guidance (currently 'Inspecting e-Safety in schools,' September 2013).
- The e-Safety audit, included in the Appendix
- Record of any incidents that have occurred

Robert Slezak
Spring 2018

Appendices

- Internet use - Possible teaching and learning activities
- e-Safety audit
- Key Stage 1 & 2 Poster
- KS1 Acceptable Use Agreement
- KS2 Acceptable Use Agreement
- Staff Acceptable Use Agreement

Appendix
Internet use - Possible teaching and learning activities

Activities	Key e-Safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	
Using search engines to access information from a range of websites.	Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick Picsearch safesearch **Google images is not recommended unless checked previously by the teacher and only then with small group supervision**
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved email accounts. Pupils should never give out personal information. Consider using systems that provide online moderation.	Email a children's author Email Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	School website Competitions School Newsletter/Newspaper
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. (Initial and Yr Group)	School website
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	Not used currently.
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used. Must be supervised by a teacher.	City Learning Centres Museums

E-Safety Audit

This quick audit will help the Senior Leadership Team assess whether the basics of e-Safety are in place.

The school has an e-Safety Policy	**Y/N**
Date of latest update:	
The policy was agreed by governors on:	
The policy is available for staff	**Y/N**
The policy is available for parents	**Y/N**
The Designated Child Protection Coordinator is	
The e-Safety Coordinator is	
How is e-Safety training provided?	
All staff have signed an Acceptable Use Agreement.	**Y/N**
All pupils have signed an Acceptable Use Agreement.	**Y/N**
e-Safety posters are displayed in all rooms with computers.	**Y/N**
Internet access is provided by an approved educational internet service provider and complies with DfES requirements for safe and secure access.	**Y/N**
The school filtering policy has been approved by SLT.	**Y/N**
An ICT security audit has been initiated by SLT, possibly using external expertise.	**Y/N**
School personal data is collected, stored and used according to the principles of the Data Protection Act.	**Y/N**
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SLT.	**Y/N**
Have these staff attended training on the filtering and monitoring systems?	**Y/N**

Key Stage 1 Poster

Think before you click

S 

I will only use the computer when an adult allows me to

A 

I will only click on things when I know they are safe

F 

I will only send friendly and polite messages

E 

If I see something I shouldn't on a screen, I will click on Hector and then tell an adult

Key Stage 2 Poster

Think before you click

- We seek teacher permission before using the Internet.
- We tell an adult if we see anything we shouldn’t and press Hector.
- We immediately close any webpage we not sure about.
- We never give out personal information or passwords.

KS1 Pupil Acceptable Use Agreement

Think before you click

S 	**I will only use the Internet and email with an adult**
A 	**I will only click on icons and links when I know they are safe**
F 	**I will only send friendly and polite messages**
E 	**If I see something I don't like on a screen, I will always tell an adult**

My Name: My signature: Date:

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*

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 Headteacher and Governing Body.
- I will not reveal my password(s) to anyone.
- 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. (Which is currently: LGFL)
- I will only use the approved school email, school MLE 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.
- I will not download any software or resources from the internet that can compromise the network, or are not adequately licensed.
- 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 without permission.
- I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice.
- 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 or laptop 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 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 e-Safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- 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 failure to comply with this agreement could lead to disciplinary action.

User Signature

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

I agree to abide by all the points above.

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 (Headteacher / AHT)

I approve this user to be set-up.

Signature ..... Date.....

Full Name ..... (printed)