Goodmayes Primary School e-Safety Policy

(see also Computing Policy, Safeguarding & Child Protection Policy, Teaching and Learning Policy, Acceptable Use Policy, Mobile Phone & Camera Policy and Anti-Bullying Policy)

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 be in control of their online experience.

The Internet policy will operate in conjunction with other policies including those for Computing, Anti-Bullying, Teaching and Learning, Home-School Video Conferencing, Data Protection and Safeguarding & Child Protection.

1 Teaching and learning

1.1 Why Internet use is important

i. The Internet is an essential element in 21st century life in education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

ii. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.2 Internet use will enhance learning

i. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

ii. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use (see also **responsible internet use** posters on display in classrooms)

iii. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.3 Pupils will be taught how to evaluate Internet content

i. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

ii. Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2 Managing Internet Access

2.1 Information system security

i. School computer systems capacity and security will be reviewed regularly.

ii. Virus protection will be updated regularly.

iii. Security strategies will be discussed with Redbridge LA.

2.2 E-mail

i. Pupils may only use approved e-mail accounts on the school system.

ii. Pupils must immediately tell a teacher if they receive offensive e-mail.

iii. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

iv. E-mail 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.

v. The forwarding of chain letters is not permitted.

2.3 Published content and the school website

i. The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

ii. The Head teacher will take overall editorial responsibility and ensure that content is accurate, appropriate and up-to-date.

2.4 Publishing pupil's images and work

i. Pupils' full names will not be used anywhere on the Website or App, particularly in association with photographs.

ii. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, newsletters, display boards and in local newspapers. New joiners will be asked for permission on entry within the admissions form.

iii. Pupils' work can only be published with the permission of parents on the school website or on the internet.

2.5 Social networking and personal publishing

i. The school will block/filter access to social networking sites.

ii. Newsgroups will be blocked unless a specific use is approved.

iii. Pupils will be advised never to give out personal details of any kind which may identify them or their location.

iv. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. The minimum age to join all social networking sites is 13 years old or older.

v. Pupils will have discussions around social networking and sites to ensure they are aware of the safety implications.

vi. Posters will be displayed around school with social networking sites and their age limits.

2.6 LGfL J2e

i. J2e is an online environment which is used for pupils to save work and staff to maintain contact with pupils to support with this work.

ii. J2e includes J2Webby, a Blogging platform that encourages pupils to be at the heart of the learning experience and to display their work. Access to this is only through the pupils' logins. All work will be submitted to a staff member before publishing.

iii. Pupils can comment on each other's work through J2Webby but all comments have to be accepted by a member of staff for publishing.

2.7 Managing filtering

i. The school will work with the LA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

ii. If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.

iii. The IT Technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.8 Managing videoconferencing

i. A secure broadband service is provided by the School.

ii. Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

iii. Videoconferencing will be appropriately supervised for the pupils' age.

iv. Webcams connected to laptops will be disabled unless used for videoconferencing in which pupils will need a staff member to authorise enabling.

v. Videoconferencing will be used to support home learning with short meetings with teaching staff (see Home-School Video Conferencing Policy).

vi. Videoconferencing may be used for parent meetings such as Parent consultations and Curriculum meetings (see Home-School Video Conferencing Policy).

2.9 Managing emerging technologies

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

ii. Mobile phones will not be used by teaching staff or pupils during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

2.10 Protecting personal data

i. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulation (May 2018).

3 Policy Decisions

3.1 Authorising Internet access

i. The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

ii. At **Key Stage 1 and Foundation stage**, after suitable introduction to the **rules** for responsible e-safety (Appendix 1a, 1b) access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved rules on-line materials.

iii. At **Key Stage 2**, Internet access will be granted to a whole class as part of the scheme of work, after suitable introduction to the **rules** for responsible Internet use (Appendix 1c). When children first join the school, parents are required to sign to verify that the school's e-safety rules have been understood and agreed and to confirm that they take responsibility for their child abiding by these rules.

3.2 Assessing risks

i. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Redbridge LA can accept liability for the material accessed, or any consequences of Internet access.

ii. The school will **audit** ICT provision to establish if the **e-Safety policy** is adequate and that its implementation is effective (Appendix 3).

3.3 Handling e-Safety complaints

i. Complaints of Internet misuse will be dealt with by a senior member of staff.

ii. Any complaint about staff misuse must be referred to the Head teacher.

iii. Complaints of a child protection nature must be dealt with in accordance with school Child Protection procedures.

iv. Pupils and parents will be informed of the complaints procedure.

v. Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

3.4 Community use of the Internet

i. External users will be expected to adhere to the school's e-Safety Policy.

4 Communications Policy

4.1 Introducing the e-Safety policy to pupils

i. 'Think then click' posters for the relevant key stage will be posted in all networked rooms/classrooms and discussed with the pupils at the start of each year (Appendix 1a and 1b)

ii. Pupils will be informed that network and Internet use will be monitored.

4.2 Staff and the e-Safety policy

i. All staff will be given the School e-Safety Policy and its importance explained.

ii. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential. (See Acceptable Use Policy – link)

4.3 Enlisting parents' support

i. Parents' attention will be drawn to the School e-Safety Policy on the school website.

4.4 Writing and reviewing the e-Safety policy

i. The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for Computing, Teaching and Learning, Anti-Bullying and for Child Protection.

ii. The school will appoint an e-Safety Coordinator. This may be the designated Child Protection Coordinator as the roles overlap.

iii. The e-Safety Policy and its implementation will be **reviewed in the Autumn Term 2024 or sooner if necessary.**

Approved by Governors: **Autumn Term 2022**

To be reviewed: **Autumn Term 2024**

L.	A. K. Garland
Interim Headteacher	**Safeguarding Governor**

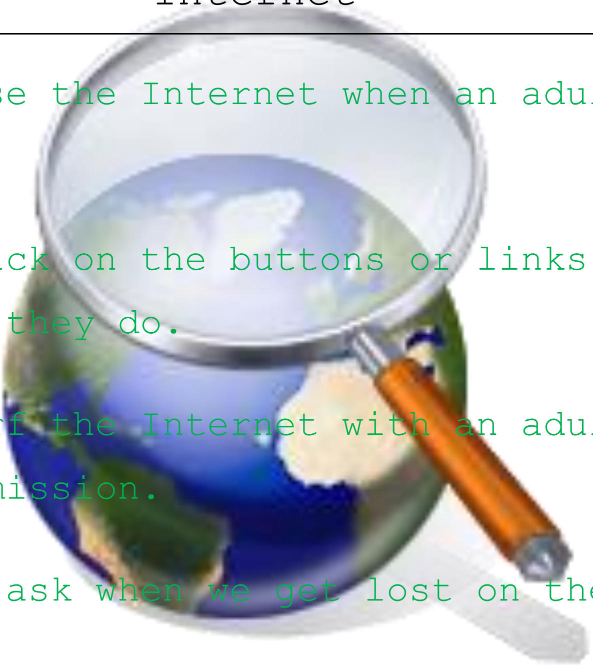
Appendix 1a

Foundation Stage

Think then Click

These rules help us to stay **safe** on the Internet

- We only use the Internet when an adult is with us.
- We can click on the buttons or links when we know what they do.
- We can surf the Internet with an adult or with their permission.
- We always ask when we get lost on the Internet.
- We can go into ‘favourites’ and play a game.

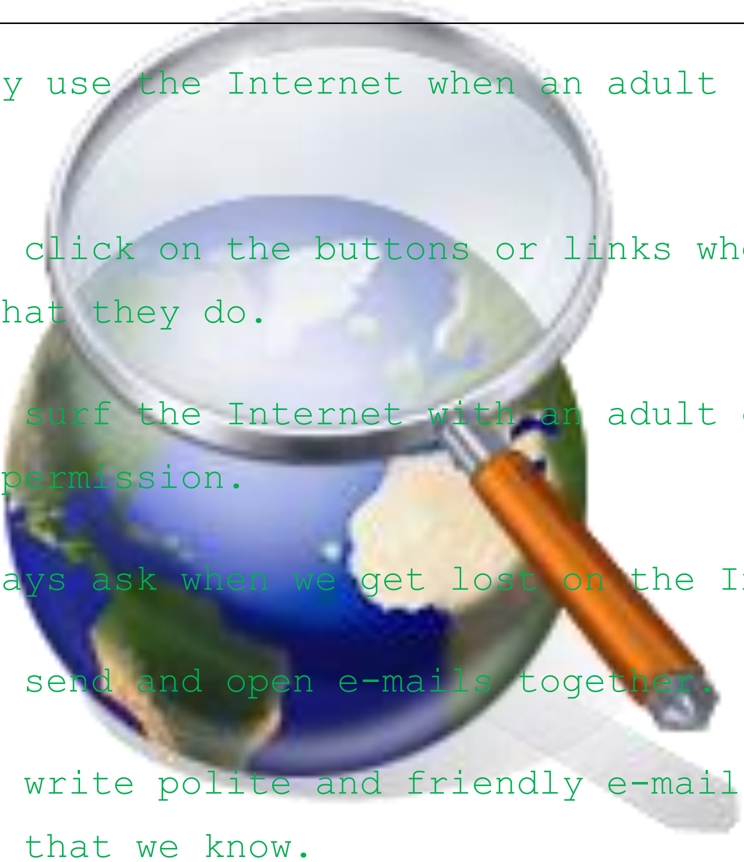


Appendix 1b

Key Stage 1

Think then Click

These rules help us to stay **safe** on the Internet



- We only use the Internet when an adult is with us.
- We can click on the buttons or links when we know what they do.
- We can surf the Internet with an adult or with their permission.
- We always ask when we get lost on the Internet.
- We can send and open e-mails together.
- We can write polite and friendly e-mails to people that we know.

TOGETHER WE CAN ACHIEVE EXCELLENCE

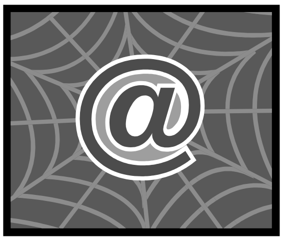
Appendix 1c

Key Stage 2

Think then Click

These rules help us to stay **safe** on the Internet

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms or social networking sites.



Appendix 2: Internet use - Possible teaching and learning activities

Activities	**Key e-safety issues**	**Relevant websites**
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. LGFL J2e Favourites list
Using search engines to access information from a range of websites.	Parental consent should be sought. 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. - CBBC Search - Google
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. J2e	2simple email E-mail a children's author E-mail Museums and Galleries E-mail children in other countries LGFL- email
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.	LGfL J2e School Website J2Webby
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.	LGFL J2e School Website Museum sites, etc. Digital Storytelling BBC – Primary Art
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.	Zoom Skype
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.	Skype Zoom National Archives "On-Line" Global Leap NaturalHistoryMuseum ImperialWarMuseum International calls

e-Safety Audit

(Appendix 3)

This quick self-audit will help the Senior Leadership Team (SLT) assess whether the e-Safety basics are in place to support a range of activities that might include those detailed within Appendix 3.

Has the school an e-Safety Policy that complies with CFE guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Has e-Safety training been provided for both students and staff?	Y/N
Do all staff sign a Computing Code of Conduct on appointment?	Y/N
Have school e-Safety rules been set for students?	Y/N
Are these rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access (e.g. the Redbridge Community Network).	Y/N
Has a computing security audit has been initiated by the SLT, possibly using external expertise?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N

Display near computers