

Online Safety policy

At Townsend Primary School we believe that we have a duty to provide pupils with quality Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills.

We believe that when used correctly Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the school's management information and business administration systems.

We acknowledge that the increased provision of the Internet inside and outside of school brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate Internet information and to take care of their own safety and security.

Online Safety, which encompasses Internet technologies and electronic communications, will educate pupils about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.

Aims

- To ensure that staff and pupils make use of the internet and other technologies for appropriate professional and educational purposes. This includes use of e-mail, World Wide Web and educational conferencing forums.
- To ensure that Internet and use of related technologies is monitored and managed appropriately.
- To provide a mechanism by which staff and pupils are protected from sites, information, and individuals that could undermine the principles and aims of the school
- To provide rules which are consistent and in agreement with the Data Protection Act and with acceptable procedures commonly used on the internet, including those associated with netiquette.
- To provide a structure for the teaching of an Online Safety module of work for all users.

Role of the Governing Body

The Governing Body has:

- appointed a member of staff to be the Coordinator for Online Safety;
- delegated powers and responsibilities to the Headteacher to ensure all school personnel and visitors to the school are aware of and comply with this policy;
- responsibility for ensuring funding is in place to support this policy;
- responsibility for ensuring policies are made available to parents;
- nominated a link governor to visit the school regularly, to liaise with the coordinator and to report back to the Governing Body;
- undertaken training in order to understand Online Safety issues and procedures;
- responsibility for the effective implementation, monitoring and evaluation of this policy

Role of the Head teacher

The Head teacher will:

- ensure all school personnel, pupils and parents are aware of and comply with this policy;

- work with the Governing Body and the Online Safety Coordinator to create a safe ICT learning environment by having in place:
 - an effective range of technological tools
 - clear roles and responsibilities
 - safe procedures
 - a comprehensive policy for pupils, staff and parents;
- monitor the effectiveness of this policy;
- annually report to the Governing Body on the success and development of this policy

Role of the Online Safety Coordinator

The Online Safety Coordinator is co-opted onto the Safeguarding Team (Simon Bartlett) (Harriet Ward)

- ensure that all Internet users are kept up to date with new guidance and procedures;
- have editorial responsibility of the school Web site and will ensure that content is accurate and appropriate;
- monitor the implementation of this policy and its effectiveness
- monitor Online Safety incident log that will be kept in the school office
- to ensure any reporting problems with the filtering system are dealt with appropriately
- to safeguard the wireless encryption key known only to Safeguarding Team
- To ensure all Anti- Virus software is updated on all devices

Role of the Nominated Governor

The Nominated Governor will:

- work closely with the Headteacher and the coordinator;
- ensure this policy and other linked policies are up to date;
- ensure that everyone connected with the school is aware of this policy;
- report to the Governing Body every term;
- annually report to the Governing Body on the success and development of this policy

Role of School Staff

School Staff will:

- comply with all the afore mentioned aspects of this policy;
- accept the terms of and sign the staff 'Acceptable Use Agreement'
- be responsible for promoting and supporting safe behaviours with pupils and Online Safety procedures;
- ensure that the use of Internet derived materials complies with copyright law;
- undertake appropriate training
- To ensure mobile are only used in designated areas (staffroom or offices)

Role of Pupils

Pupils will be aware of and comply with this policy and will be taught to:

- be critically aware of the materials they read;
- validate information before accepting its accuracy;
- acknowledge the source of information used;
- use the Internet for research;
- respect copyright when using Internet material in their own work;

- report any offensive e-mail
- To ensure all mobile phones are given in to the school office and not taken into class

Role of Parents/Carers

Parents/carers will:

- be aware of and comply with this policy
- be asked to support the Online Safety policy and to sign the consent form allowing their child to have Internet access;
- make their children aware of the Online Safety policy
- When in school parents will be advised to turn off mobiles or have them on silent

Internet Use

The school Internet access will:

- be designed for pupil use;
- include filtering provided by the Local Authority; (Atomwide)
- include filtering appropriate to the age of pupils;
- be reviewed and improved

Authorising Internet Access

- Before using any school ICT resource, all pupils and staff must read and sign the 'Acceptable ICT Use Agreement'.
- Parents must sign a consent form before their child has access to the Internet.
- All up to date records will be kept of all pupils and school personnel who have Internet access.

E-mail

Pupils must:

- only use approved e-mail accounts;
- report receiving any offensive e-mails;
- not divulge their or others personal details;
- not arrange to meet anyone via the e-mail;
- seek authorisation to send a formal e-mail to an external organisation
- KS2 Pupils must read, understand and sign the 'Pupil Acceptable Use Agreement'.
- KS1 Pupils will be made aware of the Think before 'You click Poster' which will be displayed in all KS1 classrooms. (see appendix for take home version)

School Website

Contact details on the website will be:

- the school address
- e-mail address
- telephone number

The school website will not publish:

- staff or pupils contact details;
- the pictures of children without the written consent of the parent/carer;
- the names of any pupils who are shown;
- children's work without the permission of the pupil or the parent/carer

Social Networking and Personal Publishing

Pupils will not be allowed access:

- to social networking sites except those that are part of an educational network or approved Learning Platform;
- to newsgroups unless an identified need has been approved

Netiquette

Netiquette is a term referring to good behaviour while connected to the Internet. Netiquette is mainly referring to behaviour while using Internet facilities such as individual Web sites, emails, newsgroups, message boards, chat rooms or Web communities.

The following rules, for staff and pupils, will ensure that we are well mannered when communicating electronically:

- Do not use someone else's name and pretend to be them.
- Do not try to obtain someone else's password.
- Do not call anyone names or threaten them with personal violence.
- Never forget that the person reading your mail is, indeed, a person, with feelings that can be hurt.
- Do not send anonymous messages.
- Write clearly and succinctly.
- Do not forward chain letters or unsolicited e-mails.
- Do not attach large files unless absolutely necessary.
- Do not use capital letters in messages (this is considered shouting).
- Proof read before you send.
- Check your e-mails regularly.
- Acknowledge that you have received a document.

Adult Code of Conduct for Safe Use of technology

Protect yourself

Mobile phone use:

- Only use your phone during school breaks
- Switch off your phone and store in your locker.
- Never phone parents or school agencies from your own phone
- Never take photos of children with your phone
- Never give your phone number to children or parents
- Never send text messages about children or their parents on your phone

Computer safety:

- Never tell children your personal e-mail address

- Never communicate with children on social networking sites
- Never send photos of children on the net
- Always send confidential information (i.e. with children's names) on the school's secure e-mailing system
- Never keep photos or films of children on your stick
- Do not keep confidential information on your stick
- Do not allow children in your care to have unsupervised access to computers

Camera use:

- Always use a school camera to take photos of children
- Never take a school camera home
- Always remove past photos from a school camera before taking it on a trip
- Do not allow non staff access to our photos without express permission from the parents, in writing and through the Headteacher
- Do not allow non staff to photograph our children without written permission from parents given through the Headteacher.

How complaints regarding Online Safety will be handled

The school will take all reasonable precautions to ensure Online Safety. However, owing to the size and nature of the internet, the availability of mobile technologies and the speed at which technologies change, it is not possible to guarantee that unsuitable material will never appear on a school website. Neither the school nor the authority can accept liability for material assessed in school, nor any consequences of Internet access.

Our Online Safety coordinator and the Headteacher acts as first point of contact for any complaint. The Headteacher will deal with all complaints of Internet misuse by school personnel.

Sanctions will include:

- Internet use only allowed with an adult's supervision
- Ban from using the internet for a time
- E-mail account withdrawn
- Discussion with Headteacher
- Informing parents or carers
- Referral to LA/police.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA procedures.

Online Safety Education

Units of work focusing on Online Safety are taught in KS1 and KS2 to raise the awareness and importance of safe and responsible use of the internet and related technologies. The children will be taught rules that will help to protect them when using the internet at school home at home. Online Safety rules will be on display in the ICT suite.

All lesson plans are from the CEOP's (Child Exploitation and Online Protection) website 'thinkuknow'

As part of other learning in Citizenship and PHSCE children will be supported in making informed and appropriate choices if they encounter people and material online that may be challenging, prejudiced,

inaccurate or that promote an extreme lifestyle or point of view. Accessing violent extremist websites, especially those with a social networking element. (Please refer to our Safeguarding Policy)
The school uses DfE guidelines and LA resources to support this – eg the Southwark PREVENT team.

Inappropriate Material

Any inappropriate websites or material found by pupils or school personnel will be reported to the Online Safety Coordinator who in turn will report to the Internet Service Provider.

Prevent Duty and Extremism

DfE PREVENT Duty

'The Prevent duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities, in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism'

<https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty>

The school uses DfE guidelines and resources provided by Southwark LA to support this aspect of safeguarding.

See the Safeguarding policy for more information

Extremism online

As part of other learning in Citizenship and PHSE children will be supported in making informed and appropriate choices if they encounter people and material online that may be challenging, prejudiced, inaccurate or that promote an extreme lifestyle or point of view.

Educate against Hate (DfE/Home Office)

<http://educateagainsthate.com/>

Internet System Security

- New programs will be installed onto the network or stand alone machines by Local Authority technicians.
- Personal memory sticks, CD's and other data recording devices may not be used in school.
- Everyone must be aware that under the Computer Misuse Act 1990 the use of computer systems without permission or for inappropriate use could constitute a criminal offence.

Complaints

- The Headteacher will deal with all complaints of Internet misuse by school personnel or pupils.
- Parents will be informed if their child has misused the Internet

Raising Awareness of this Policy

We will raise awareness of this policy via:

- Annual Online Safety day
- the school website
- the Staff Handbook

- meetings with parents such as introductory, transition, parent-teacher consultations and periodic curriculum workshops
- meetings with school personnel
- communications with home such as weekly newsletters and of end of half term newsletters
- reports such annual report to parents and Headteacher reports to the Governing Body

Monitoring the Effectiveness of the Policy

The effectiveness of this policy will be reviewed by the coordinator, the Headteacher and the nominated governor on an annual basis. In line with new technologies the necessary recommendations for improvement will be made to the Governors.

Townsend Primary School

Parental consent form – Use of ICT in school

Parent/Guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above named pupil(s), I grant permission for my daughter or son to have access to use the internet, e-mail and other ICT facilities at school.

I know my daughter or son has signed an Online Safety agreement form and that they have access to, and are taught, the 'rules' for responsible ICT use.

I accept that ultimately the school cannot be held responsible for the nature and content of the materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access e-mail, employing appropriate teaching practice and teaching Online Safety skills to pupils.

I understand that the school can check my child's computer files, and the internet sites they visit, and that if they have concerns about my child's Online Safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's Online Safety.

Parent / guardian signature: _____

Date; ____/____/____

Townsend Primary School

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 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.

- 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.

Name of Staff _____

Signature _____ Date _____

Townsend Primary School

Name _____

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: _____

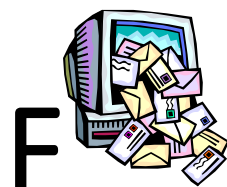
Think before you click



I will only use the Internet and email with an adult



I will only click on icons and links when I know they are safe



I will only send friendly and polite messages

Appendix

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
Year 1	Using Technology Safely <ul style="list-style-type: none"> Communicating Online Personal Information Staying Safe/Getting Help 	Coding and Programming <ul style="list-style-type: none"> Programming on screen Sequence, Repetition and Selection Programming Languages De-bugging 	Understanding Technology <ul style="list-style-type: none"> Understanding Networks The Internet 	Robots Sensors and Control <ul style="list-style-type: none"> Interacting with technology Sensors/Data logging Robots Building/programming physical systems Flow diagrams 	Using Technology Safely <ul style="list-style-type: none"> Social Networking Being Responsible Reporting Concerns 	Computer Games <ul style="list-style-type: none"> Creating computer games De-bugging - Identifying and correcting errors Problem Solving and improvement
	Coding and Programming <ul style="list-style-type: none"> Algorithms/Decomposition 		Robots Sensors and Control <ul style="list-style-type: none"> Real world control systems Impact of tech on society 		Computer Games <ul style="list-style-type: none"> Playing and analysing games 	
Year 2	Using Technology Safely <ul style="list-style-type: none"> Communicating Online Personal Information Staying Safe/Getting Help 	Coding and Programming <ul style="list-style-type: none"> Programming on screen Sequence, Repetition and Selection Programming Languages De-bugging 	Understanding Technology <ul style="list-style-type: none"> Understanding Networks The Internet 	Robots Sensors and Control <ul style="list-style-type: none"> Interacting with technology Sensors/Data logging Robots Building/programming physical systems Flow diagrams 	Using Technology Safely <ul style="list-style-type: none"> Social Networking Being Responsible Reporting Concerns 	Computer Games <ul style="list-style-type: none"> Creating computer games De-bugging - Identifying and correcting errors Problem Solving and improvement
	Coding and Programming <ul style="list-style-type: none"> Algorithms/Decomposition 		Robots Sensors and Control <ul style="list-style-type: none"> Real world control systems Impact of tech on society 		Computer Games <ul style="list-style-type: none"> Playing and analysing games 	
Year 3	Using Technology Safely <ul style="list-style-type: none"> Communicating Online Personal Information Staying Safe/Getting Help 	Coding and Programming <ul style="list-style-type: none"> Programming on screen Sequence, Repetition and Selection Programming Languages De-bugging 	Using Technology Safely <ul style="list-style-type: none"> Social Networking Being Responsible Reporting Concerns 	Computer Games <ul style="list-style-type: none"> Creating computer games De-bugging - Identifying and correcting errors Problem Solving and improvement 	Understanding Technology <ul style="list-style-type: none"> Understanding Networks The Internet 	Robots Sensors and Control <ul style="list-style-type: none"> Interacting with Technology Sensors/Data logging Robots Building/programming physical systems Flow diagrams
	Coding and Programming <ul style="list-style-type: none"> Algorithms/Decomposition 		Computer Games <ul style="list-style-type: none"> Playing and analysing games 		Robots Sensors and Control <ul style="list-style-type: none"> Real world control systems Impact of tech on society 	
Year 4	Using Technology Safely <ul style="list-style-type: none"> Communicating Online Personal Information Staying Safe/Getting Help 	Coding and Programming <ul style="list-style-type: none"> Programming on screen Sequence, Repetition and Selection Programming Languages De-bugging 	Using Technology Safely <ul style="list-style-type: none"> Social Networking Being Responsible Reporting Concerns 	Computer Games <ul style="list-style-type: none"> Creating computer games De-bugging - Identifying and correcting errors Problem Solving and improvement 	Understanding Technology <ul style="list-style-type: none"> Understanding Networks The Internet 	Robots Sensors and Control <ul style="list-style-type: none"> Interacting with technology Sensors/Data logging Robots Building/programming physical systems Flow diagrams
	Coding and Programming <ul style="list-style-type: none"> Algorithms/Decomposition 		Computer Games <ul style="list-style-type: none"> laying and analysing games 		Robots Sensors and Control <ul style="list-style-type: none"> Real world control systems Impact of tech on society 	
Year 5	Using Technology Safely <ul style="list-style-type: none"> Communicating Online Personal Information Staying Safe/Getting Help 	Coding and Programming <ul style="list-style-type: none"> Programming on screen Sequence, Repetition and Selection Programming Languages De-bugging 	Understanding Technology <ul style="list-style-type: none"> Understanding Networks The Internet 	Robots Sensors and Control <ul style="list-style-type: none"> Interacting with technology Sensors/Data logging Robots Building/programming physical systems Flow diagrams 	Using Technology Safely <ul style="list-style-type: none"> Social Networking Being Responsible Reporting Concerns 	Computer Games <ul style="list-style-type: none"> Creating computer games De-bugging - Identifying and correcting errors Problem Solving and improvement
	Coding and Programming <ul style="list-style-type: none"> Algorithms/Decomposition 		Robots Sensors and Control <ul style="list-style-type: none"> Real world control systems Impact of tech on society 		Computer Games <ul style="list-style-type: none"> Playing and analysing games 	
Year 6	Using Technology Safely <ul style="list-style-type: none"> Communicating Online Personal Information Staying Safe/Getting Help 	Coding and Programming <ul style="list-style-type: none"> Programming on screen Sequence, Repetition and Selection Programming Languages De-bugging 	Understanding Technology <ul style="list-style-type: none"> Understanding Networks The Internet 	Robots Sensors and Control <ul style="list-style-type: none"> Interacting with technology Sensors/Data logging Robots Building/programming physical systems Flow diagrams 	Using Technology Safely <ul style="list-style-type: none"> Social Networking Being Responsible Reporting Concerns 	Computer Games <ul style="list-style-type: none"> Creating computer games De-bugging - Identifying and correcting errors Problem Solving and improvement
	Coding and Programming <ul style="list-style-type: none"> Algorithms/Decomposition 		Robots Sensors and Control <ul style="list-style-type: none"> Real world control systems Impact of tech on society 		Computer Games <ul style="list-style-type: none"> Playing and analysing games 	