Days Lane Primary School

E-Safety Policy

Days Lane E-Safety Policy

Aims

This policy sets out the ways in which the school will:

- Educate all members of the school community on their rights and responsibilities with the use of technology;
- Build both an infrastructure and culture of e-safety;
- Work to empower the school community to use the Internet as an essential tool for life-long learning.

The E-safety policy will be reviewed annually and will be under continuous revision in response to significant new developments in the use of technologies, new threats to esafety or incidents that have taken place.

Scope of Policy

This policy applies to all members of the school community, including staff, pupils, volunteers, parents/carers, visitors and community users.

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 such as cyber-bullying, which may take place out of school, but are linked to membership of the school.

The school will manage e-safety as described within this policy and associated positive behaviour policy, and will inform parents and carers of known incidents of inappropriate e-safety behaviour that take place in and out of school.

Roles and Responsibilities

Role	Responsibilities
Governors	□ Approve and review the effectiveness of the E-safety Policy □ Delegate a governor to act as e-safety link *(Mrs Govier)* □ E-safety Governor works with the e-safety Leader to carry out regular monitoring and report to Governors
Head Teacher and Senior Leaders	□ Ensure that all staff receive suitable CPD to carry out their e-safety roles □ Create a culture where staff and learners feel able to report incidents □ Ensure that there is a progressive e-safety curriculum in place □ Ensure that there is a system in place for monitoring e-safety □ Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff or pupil □ Inform the local authority about any serious e-safety issues □ Ensure that the school infrastructure/network is as safe and secure as possible □ Ensure that policies and procedures approved within this policy are implemented □ Use an audit to annually review e-safety with the school's technical support *(360 degree review)*
E-safety Leader	□ Log, manage and inform others of e-safety incidents and how they have been resolved where this is appropriate □ Lead the establishment and review of e-safety policies and documents □ Lead and monitor a progressive e-safety curriculum for pupils □ Ensure all staff are aware of the procedures outlined in policies relating to esafety □ Provide and/or broker training and advice for staff □ Attend updates and liaise with the LA e-safety staff and technical staff □ Meet with Senior Leadership Team and e-safety Governor to regularly discuss incidents and developments □ Coordinate work with the school's designated Child Protection Officers

Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website, in the staffroom, in classrooms and electronically on the shared staff drive
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year
- Acceptable use agreements to be issued to whole school community, usually on entry to the school

Handling Complaints:
The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

- Discussion with Leader of Learning / members of the Senior Leadership Team / Head teacher □Informing parents or carers
- Removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system
- Referral to LA / Police
- Our E-Safety Leader acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.
- Complaints of cyberbullying are dealt with in accordance with our Positive Behaviour Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring
The e-safety policy is referenced from within other school policies: Safeguarding and Child Protection policy, Positive Behaviour policy and the School Development Plan.

- The school has an e-safety leader who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed regularly or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the Head teacher and E-safety Leader and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the Senior Leadership Team and approved by Governors. All amendments to the school esafeguarding policy will be discussed in detail with all members of teaching staff.

E-safety curriculum at Days Lane Primary School

Has a clear, progressive e-safety education programme as part of the Computing curriculum/PSCHE curriculum. It is built on national guidance and uses the 'Education for a Connected World Framework' (published by UKCCIS) to outline skills and understanding that children develop at different ages and stages throughout the school. It highlights what a child should know in terms of current technology, its influence in behaviour and development, and what skills are needed to be able to navigate it safely. It focusses on eight different aspects of online education:

1. **Self-images and Identity:** The differences between offline and online identities and identifies effective routes for reporting and support, as well as exploring the impact of online technologies on behaviour.
2. **Online Relationships:** How technology shapes communicating styles and identifies strategies for positive relationships in online communities.
3. **Online Reputation:** Exploring the concept of reputation and how others may use online information to make judgements.
4. **Online Bullying:** Exploring bullying and other online aggression and how technology impacts those issues.
5. **Managing Online Information:** How online information is found, viewed and interpreted e.g. learning to search effectively online and publish ethically.
6. **Health, Well-being and Lifestyle:** The impact technology has on health, well-being and lifestyle.
7. **Privacy and Security:** How personal online information can be used, stored, processed and shared.
8. **Copyright and Ownership:** Exploring the concept of ownership and online content and using strategies to protect personal content.

Staff and Governor Training

Days Lane Primary School:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection (e.g. by using Egress);
- Makes regular training available to staff on e-safety issues and the school's esafety education program.
- Provides, as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policy.

Parent Awareness and Training:

- Runs a rolling programme of advice, guidance and training for parents, including:
- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
- Information leaflets; in school newsletters; on the school web site ○ E-safety

  workshops, led by the borough Public Health Advisor for Children ○

Suggestions for safe Internet use at home ○ Provision of information about national support sites for parents.

Data Protection

- We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998 and is fully compliant with GDPR regulations.
- Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- All computers, throughout the school, are set to screen lock after 5 minutes. A user password is then required to return to the previous screen/ document.
- Teacher's login passwords are automatically set to be updated/ changed three times a year.
- Staff will not remove personal or sensitive data from the school premises without permission of the Head teacher.
- Teachers must not use memory keys or portable hard drives to store information on. They must use Microsoft One Drive, which stores saved information in the cloud and can only be accessed with a member of staff's Windows 365 username and password.

Incident Management Expected Conduct

In this school, all users:

- Are responsible for using the school IT systems in accordance with the relevant Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying

Staff

- Are responsible for reading the school's E-safety policy and using the school IT systems accordingly, including the use of mobile phones, and hand held devices.
- They model safe and responsible behaviour in their own use of technology.
- Refer to the 'rules of appropriate use' with children on an a termly basis and reiterate what sanctions result from misuse.

Pupils

- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the E-safety acceptable use agreement form at the time of their child's entry to the school.
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management

At Days Lane Primary School:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's positive behaviour processes (see Positive Behaviour policy).
- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- Monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school.
- Parents/carers are specifically informed of e-safety incidents involving their child, for whom they are responsible.
- We will contact the Police if any of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

Managing the ICT infrastructure: Internet access, security (virus protection) and filtering

Days Lane Primary School:

- Has the educational filtered secure broadband connectivity through Exa Networks (SurfProtect) – https://surfprotect.co.uk/
- Blocks all chat rooms and social networking sites
- Only unblocks other sites for specific purpose, agreed by the Head teacher.
- Has blocked pupil access to music download or shopping sites
- Is vigilant in its supervision of pupils' use at all times (as far as is reasonable)
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the school's website and internal folders.
- Requires staff to preview websites before use (where not previously viewed or cached); Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;

- Informs all users that Internet use is monitored;
- Informs staff and pupils that that they must report any failure of the filtering systems directly to the person responsible for URL filtering. Our system administrator(s) logs or escalates as appropriate to our Technical service provider (JSPC);
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities; Police, and the LA.

Email pupils:

- Pupils are introduced to, and use e-mail as part of the Computing scheme of work.
- Pupils cannot receive external emails and are taught emailing using a secure site (2 Email - Purple Mash)
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
- not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
- that an e-mail is a form of publishing where the message should be clear, short and concise;
- that any 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;
- They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- that they should think carefully before sending any attachments; ○ embedding adverts is not allowed;
- that they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages; ○ not to delete malicious of threatening e-mails, but to keep them as evidence of bullying; ○ not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them; ○ That forwarding 'chain' e-mail letters is not permitted.

Email Staff:

- Staff can only use the 365 email system
- Staff only use the 365 email system for professional purposes
- Staff must not access their personal email accounts on any IT equipment e.g. laptops, Ipads, stand-alone computers
- Never use email to transfer staff or pupil personal data. Members of the SLT must use secure, LA / DfE approved systems (Egress).

School Website

- The Head teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to a limited number of users as agreed by the Head teacher:
- Deputy Head Teacher
- Esafety Leader
- Office Manager ○ The school web site complies with the statutory DfE guidelines for publications; ○ Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images

Social Networking (See the school's Social Media Policy for further information)

Teachers are instructed not to run social network spaces for pupils use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in any online discussion on personal matters relating to the running of the school or members of the school community e.g. through social media networks such as Facebook and WhatsApp.
- Personal opinions should not be attributed to the school or local authority ○ In the event that staff do not adhere to the above expectations, it is likely to result in disciplinary action.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Equipment and Digital Content

Personal mobile phones and mobile devices
Staff use of Personal Devices

- Only the Head Teacher and non-teaching Senior Leaders should have access to their phones at all times in case of an emergency.
- Staff mobile phones and personally-owned devices will be switched off or switched to 'silent' mode and stored in the classroom safes during the school day. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used **during teaching periods** unless permission has been agreed in advance by a member of the Senior Leadership Team (in emergency circumstances only). In such circumstances, staff should use their mobile phones during break times in a private space away from children e.g. staff room, toilets or classroom with no children and the door closed.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Staff recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Head teacher. Such authorised use is to be monitored and recorded.
- All mobile phone use is to be open to scrutiny and the Head teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- If a member of staff breaches the school policy then disciplinary action is likely to be taken.
- During school journeys and residential trips, staff will be issued with a school phone to contact parents or carers if required.
- In emergency situations where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.

Pupils use of Personal Devices

The School permits children in Year 6, who walk home without adult supervision, to bring a mobile phone into school. Parents are sent the school's mobile phone expectations and must sign a permission form, in order for their child to be able to bring their mobile phone into school:

Year 6 Mobile Phone Expectations

1) *Pupils are not permitted, under any circumstances, to use their mobile phones whilst on school premises.*
2) *Pupils must keep mobile phones in their school bags until they are brought into the classroom at the start of registration.*
3) *For safe keeping, the mobiles will be stored in a class box in the office during the day and will be returned by the class teacher at the end of the day.*
4) *Parents are not allowed to contact their child via their mobile phone during the school day, but to contact the school office.*
5) *If any child is found to be using their phone in an inappropriate manner, it will be confiscated and returned to parents. This may result in withdrawing permission for them to bring their phone into school again.*
6) *Please be aware that the school is not responsible for the loss, theft or damage to any mobile phone and children bring them into school at their own risk.*
7) *If parents/ carers give consent for their child to walk home from school unsupervised, and they would like them to bring their mobile phones into school, they must read the above expectations and complete a permission form, which is sent via Parent Mail.*

- Where parents or pupils need to contact each other during the school day, they should do so only through the School Office.
- The School accepts that there may be particular circumstances in which a parent of a child (outside of Year 6) wishes their child to have a mobile phone for their own safety and this needs to be agreed in advance in writing to the Head teacher.

Digital images and video in school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the data collection form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications, the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of the computing curriculum.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

<u>Cyberbullying</u>

- Childnet International: www.childnet.com
- Digizen: www.digizen.org
- Internet Watch Foundation: www.iwf.org.uk
- Think U Know: www.thinkuknow.co.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Anti-Bullying Alliance: www.anti-bullyingalliance.org.uk
- Beat Bullying: www.beatbullying.org
- ChildLine: www.childline.org.uk

<u>Sexting</u>

Sexting: responding to incidents and safeguarding children
https://www.safeguardinginschools.co.uk/wp-content/uploads/2016/08/Sexting-in-schoolsand-colleges-UKCCIS-August-2016.pdf

Completed: July 2019 Review Date: July 2021

Appendix A: Acceptable Use Agreements (EYFS, KS1 & KS2)

Dear Parents/ Carers

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Parent / Carer Signature

As the parent / carer, I understand that the school has discussed the Acceptable Use Agreement with my son /daughter as part of whole school commitment to e-Safety both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet.

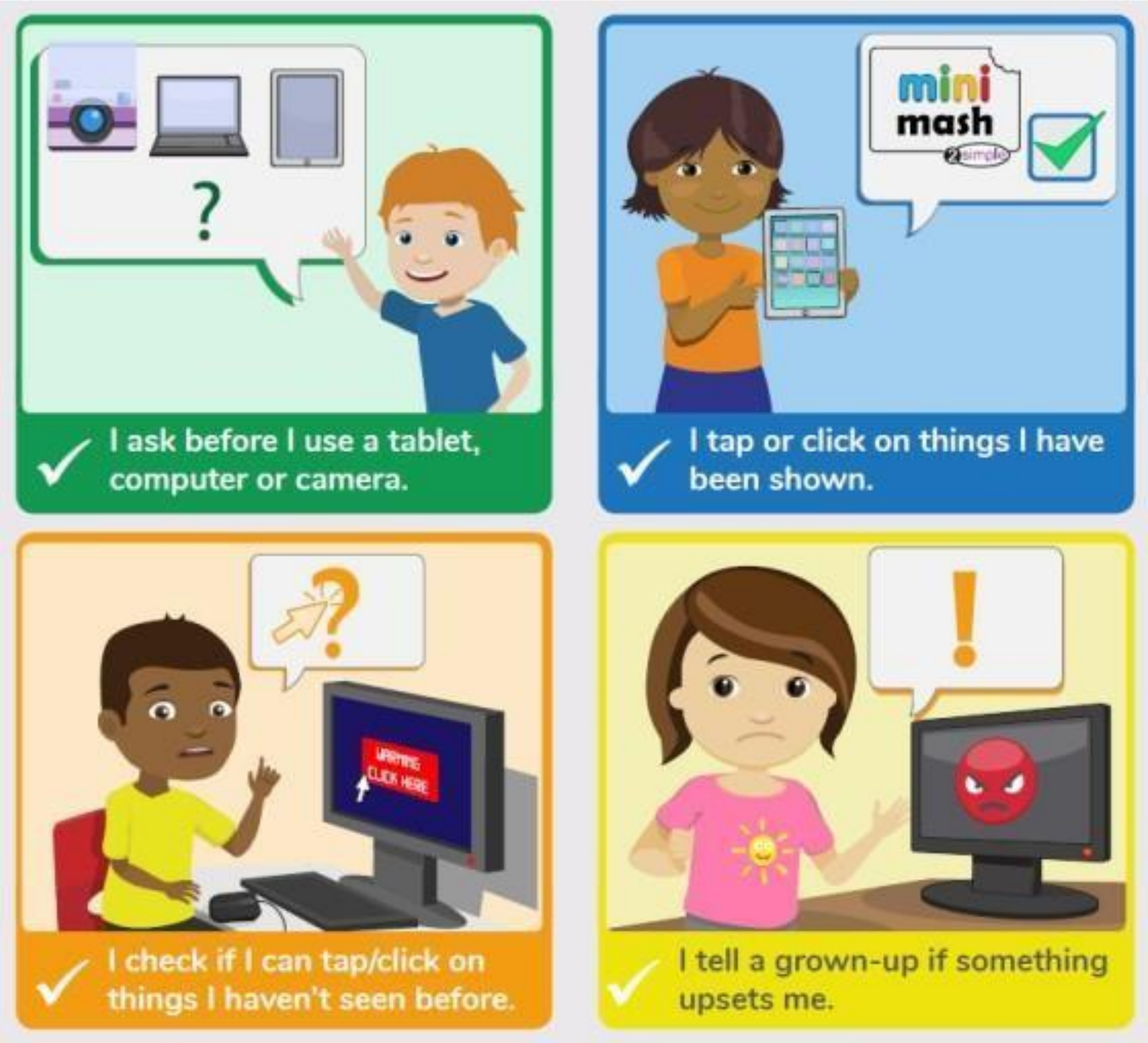
I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Name of Pupil ________________________________ Class _______________

Signed (parent) _______________________________ Date _______________

Acceptable Use Agreement

EYFS


?
mini mash
2simple
✓ I ask before I use a tablet, computer or camera.
✓ I tap or click on things I have been shown.
?
WARNING CLICK HERE
!
✓ I check if I can tap/click on things I haven't seen before.
✓ I tell a grown-up if something upsets me.

My Name: ______________________________

Parent/ Carer Signed: ________________________

Date: __________________

Acceptable Use Agreement

KS1

- I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- I only open activities that an adult has told or allowed me to use.
- I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- I keep my passwords safe and will never use someone else's.
- I know personal information such as my address and birthday should never be shared online.
- I know I must never communicate with strangers online.
- I am always polite when I post online, use an email and other communication tools.

I understand this agreement and know the consequences if I don't follow it.

My Name: _________________________________ Parent/

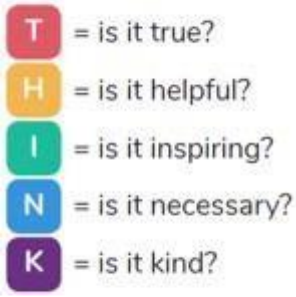
Carer Signed: _______________________

Date: _____________________________________

Acceptable Use Agreement

KS2

- I will only access computing equipment when a trusted adult has given me permission and is present.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- Before I share, post or reply to anything online, I will T.H.I.N.K.



T = is it true?

H = is it helpful?

I = is it inspiring?

N = is it necessary?

K = is it kind?

- I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

I understand this agreement and know the consequences if I don't follow it.

My Name: ________________________________ Parent/

Carer Signed: ______________________

Date: ____________________________________

Appendix B: ‘Rules of appropriate use’

Keeping safe: Stop, think, before you click! 12 rules for responsible ICT use

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

1) I will only use the school’s computers for schoolwork and homework.
2) I will only delete my own files.
3) I will not look at other people’s files without their permission.
4) I will keep my login and password secret.
5) I will not bring files into school without permission.
6) I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
7) I will only e-mail people I know, or my teacher has approved.
8) The messages I send, or information I upload, will always be polite and sensible.
9) I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
10) 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 my teacher has given permission.
11) I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
12) 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 tell a teacher or responsible adult.