E-Safety Policy

Document Detail	
Category:	Safeguarding
Authorised By:	Full Governing Body
Author:	Deputy Head & Computing Subject Leader
Version:	1
Approval date	December, 2016
Next Review Date:	December, 2019
To be read in conjunction with:	REAch2 Social Media Policy, REAch2 Freedom of Information & Data Protection Policy & Procedure

Tidemill's E-Safety and Acceptable Use Policy

E-Safety encompasses internet technologies and electronic communications such as mobile phones, iPads and wireless technology. Most young people are enthusiastic Internet users - particularly of interactive services like: Email, Chat and Instant Messaging. However, like many exciting activities, there are risky situations to deal with and hazards to avoid. Robust policies and procedures, clear roles and responsibilities, a comprehensive e-safety education programme for pupils, staff and parents and an effective range of technological tools to support e-safety are essential to providing a safe ICT learning environment.

Context

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.
To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant messaging / video messaging (e.g. Facetime) using simple web cams
- Blogs (an online interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (www.facebook.com)
- Video broadcasting sites (www.youtube.com)
- Chat Rooms (www.teenchat.com)
- Gaming Sites (www.minecraft.com)
- Music download sites (Spotify)
- Smart phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.
- Tablets and iPads
- Apps (such as Whatsapp and Kik)

Tidemill uses the National Curriculum for Computing and integrates it within the International Primary Curriculum. E-safety is embedded across the three strands of the National Curriculum (Digital Literacy, Computer Science and Information Technology). Children should apply their ICT knowledge, skills and understanding confidently and competently in their learning and in everyday contexts and become independent and discerning users of technology, recognising opportunities and risks and using strategies to stay safe. This is embedded in Computing lessons, PSHE circle times and weekly e-safety scenarios.

The two E-Safety outcomes for KS1 and KS2 are:

- Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies (KS1)
- Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact (KS2)

Please see the Computing National Curriculum for a further break down of these outcomes.

Policies and Procedures

- The school's e-Safety policy will operate in conjunction with other policies including: Computing, Positive Behaviour, Anti-Bullying, Teaching and Learning and Data Protection.
- It has been approved by governors after input from staff and parents.
- The e-Safety Policy and its implementation will be reviewed annually and where necessary in cases of reported misconduct or risks.
- All Tidemill, staff and pupils are asked to sign an Acceptable Use Policy (AUP- **see Appendix**) detailing the ways staff, pupils and all network users should use our ICT facilities and reflects the need to raise awareness of the safety issues associated with electronic communications as a whole. The AUP is displayed in all classrooms.
- E-Safety will form a key part of the Computing/PSHE curriculum. Children will be made aware of the dangers and risks of using the internet and mobile technologies throughout the school year. This will include learning about issues during Anti-Bullying/Safe School Week/Safer Internet Day and will form an integral part of computing lessons.
- Digital leaders are appointed in Year 5 and Year 6 and they take increased responsibility for teaching others about e-Safety (e.g. Inspire Workshops and assemblies).
- Each week, digital leaders share an e-Safe scenario with EYFS, KS1 and KS2 and this is discussed in class.

Internet Access

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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 pupils.
- The school's Internet access is designed for pupil use and uses the Atomwide and LGfL filtering system.
- Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use. Pupils will not use the internet without having permission from a member of staff.
- Pupils will not use social networking sites (these are blocked) in school and will be educated about their safe usage in their own time. Parents will also be educated in these areas during e-Safety workshops.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. (Reference to YAPPY in KS2 will be made – Your name, address, password, phone number or your plans).

- Pupils are forbidden from downloading games or other programmes from the Internet.
- Downloading programs from the internet will be carried out by the IT Technician or ICT Leader.
- Public chat-rooms and instant messaging are not allowed and are blocked using the school internet filter.
- Access to peer-to-peer networks is forbidden in school.
- Pupils will be educated in 'Digital Literacy' and taught how to evaluate the internet content that they have located. Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught to reference materials they have found from other sources so as not to infringe copyright or the intellectual property of others.
- Pupils will be taught how to report inappropriate Internet content.

E-mail

- When available, pupils may only use approved school e-mail accounts on the school's Fronter Learning Platform. Pupils are not permitted to use their own personal email accounts on school equipment.
- Before using school e-mail accounts, children will develop an 'Essential Agreement' with guidelines on how to use email and how to stay safe.
- Pupils must immediately tell a teacher if they receive an offensive e-mail and are asked to keep the email in order to show the adult.
- In e-mail communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mails should be treated as suspicious and attachments not opened unless the author is known.
- Emails 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.
- Staff should never use personal email addresses to communicate with pupils or parents. An official school email address will be provided by the ICT Subject Leader.

Virtual Learning Environment

- The VLE is provided for use of Tidemill Academy staff and pupils only. At present, access by any other party is strictly prohibited.
- Pupils should never reveal his/her password to anyone or attempt to access the service using another pupil's login details. Pupils should inform their teacher or the Computing leader if they feel their password has been compromised.
- All staff and pupils possess a username and password as a level of security. The correct levels of privilege are applied to the correct users.
- Activity on the Learning Platform will be monitored to ensure that the content posted by users is valid and does not infringe the intellectual property rights of others.

Published content and the school website

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The Assistant Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
  Permission from parents or carers will be obtained before photographs of pupils are published. Events are organised throughout the academic year and sometimes photographs of the children are taken to use in publications, media & school information booklets/websites/Twitter. Pupils' full names will not be used anywhere on the website or blog, particularly in association with photographs. Additional permission is always sought before publishing photographs for any other use e.g. local media and news coverage.
- Pupil image file names will not refer to the pupil by name.
- Pupil image files should be securely stored on the school network.

Video Conferencing and Webcam Use

- When available, video conferencing and webcam use will be appropriately supervised.
- Pupils (and parents) will be taught the dangers of using webcams outside of school.

Portable Devices

- Children will not use mobile phones during school time and on school property. For children who walk home alone, phones must to be handed in to the class teacher at the beginning of the day.The sending of abusive or inappropriate text messages is forbidden and children are educated what to do in case this happens.
- Staff should be aware that technologies such as mobile phones can access the internet by bypassing filtering systems and present a new route to undesirable material and communications.
- Staff should not use their personal mobile phones to contact pupils or capture photographs of children. Neither should they use personal cameras to take photographs. Alternative equipment will be provided by the school.
- Pupils are taught how to protect themselves from being victims of identity theft and how to report such an event to the correct authority.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. These may not be used in school.

Protecting Personal Data

- Personal data will only be made available to appropriate and approved sources in accordance with the Data Protection Act 1998.

Role and Responsibilities

Our e-Safety Coordinator and Senior Safeguarding Officer is David Petty. Our e-Safety Coordinator ensures staff and pupils keep up to date with e-Safety issues and guidance; keeps the Headteacher, senior leaders and governors updated as necessary; ensures that all e-Safety concerns are reported to the Safeguarding Officer who will investigate the concern and take appropriate action.

Our Governor responsible for e-Safety is David Mason. Our Governors have an understanding of e-Safety issues and strategies at the school; are aware of local and national guidance on e-Safety; are updated at least annually on policy developments.

Our staff responsibilities are to be familiar with the policy and to adhere to its procedures. They should be familiar with the school's policy in regard to:

- Safe use of e-mail.
- Safe use of Internet.
- Safe use of school network, equipment and data.
- Safe use of digital images and digital technologies, such as mobile phones, digital cameras and iPads.
- Publication of pupil information/photographs and use of website.
- e-Bullying / Cyberbullying procedures.
- Their role in providing e-Safety education for pupils.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will always use a child friendly, safe search engine when accessing the internet with pupils (e.g. Google Safe Search – default settings).

Staff are to be updated about e-Safety matters at least once a year. At the start of each year, e-Safety will form part of the staff professional development day and new staff are expected to sign an AUP agreement (see appendix.)

Managing Internet Access and Other Technologies

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- All staff and pupils possess individual logons and passwords to the school network with appropriate access rights and privileges.
- Virus protection will be installed on all school computers and updated regularly in light of new viruses and Trojan Horses that weaken the schools security.
- Staff must ask permission from the e-Safety Coordinator before installing software on any school machines.

Managing filtering

- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator or the Network Manager. The website should be minimised to allow for further investigation.
- The IT Technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will give responsibility to the school technician to monitor the use of internet, email and messaging services.
- The school should audit ICT use to establish if the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate.

Handling e-Safety complaints

- Complaints of Internet misuse will be dealt with by the e-Safety/Senior Safeguarding Officer (David Petty).
- Any complaint about staff misuse must also be referred to the Senior Safeguarding Officer or Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (See Safeguarding Policy)
- Pupils and parents will be informed of the possible consequences for pupils misusing the Internet.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the police to establish procedures for handling potentially illegal issues.

Enlisting parents' support

- Parents' attention will be drawn to the school e-Safety Policy in newsletters, the school brochure and on the school website.
- Parents will be given a copy of the Acceptable Use Policy that their child has signed. They will be strongly encouraged and supported to monitor their children's use of technology at home.
- The school will provide regular e-Safety sessions for parents.

Glossary

Acceptable Use Policy: A policy that a user must agree to abide by in order to gain access to a network or the internet. In the schools context, it may also cover how other communications services, such as mobile phones and camera phones, can be used on the school premises.

Avatar: A graphic identity selected by a user to represent him/herself to the other parties in a chat-room or when using instant messaging.

Chat-room: An area on the internet or other computer network where users can communicate in real time, often about a specific topic.

Filtering: A method used to prevent or block users' access to unsuitable material on the internet.

Information Literacy: The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.

Instant messaging(IM): A type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet, analogous to a telephone conversation but using text-based, not voice-based, communication.

Peer-to-peer (P2P): A peer-to-peer network allows other users to directly access files and folders on each others computer. File sharing networks such as 'Lime Wire' create weaknesses in networks security by allowing outside users access to the schools resources.

Spam: Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

Spoofing: Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan Horses: A virus which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.

Video Conferencing: The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video.

Virus: A computer program which enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

Webcam: A webcam is a camera connected to a computer that is connected to the internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.

Appendix

Acceptable Use Policy-AUP
KS1 Pupil Agreement

TIDEMILL ACADEMY

When using the Internet

THINK BEFORE YOU CLICK

S 	I will only use the *Internet* when I have an adult's permission.
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 minimise the website and tell an adult immediately.
Wet Play 	During wet play I will **ONLY** go on these websites: EducationCity.com espresso education cbbc BBC fronter Knowledge through collaboration

I understand how to be safe when using the internet.

Class:

KS2: AUP
Rules of Acceptable Use for Computers

All children must sign the AUP before using a school computer

Acceptable Use for Technology Agreement

At Tidemill, we use a range of technology to help our learning. This agreement will keep everyone safe and help us be fair to others.

- I will I will ask permission from a member of staff before using the Internet.
- I will only access the system and Fronter with my own login and password.
- I will keep my logins and passwords secret and I will let my teacher know if I need to change my password.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will only use the computers for school work and homework.
- I will not download and use material (e.g. copy and paste) content which is copyright ©
- I will not bring in memory sticks or disks from outside school unless I have been given permission.
- I will only e-mail people I know or a responsible adult has approved using Fronter and will only use my School email account.
- The messages I send, or information I upload, will always be polite and sensible.
- 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 not open an attachment, or download a file, unless I know and trust the person who has sent it.
- 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 or a responsible adult. I understand my report would be confidential and would help protect other pupils and myself.
- 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 understand that the school may check my computer files and may monitor the Internet sites I visit.
- When using the iPads, I will only use the apps that my teacher has given me permission to use.

CLASS NAME:_____

TIDEMILL ACADEMY

Acceptable Use Policy (AUP): Staff Agreement Form

	Name of School	**Tidemill Academy**
	AUP review Date	**Autumn, 2016**
	Date of next Review	**Autumn, 2019**
	Who reviewed this AUP?	

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 follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it.
- I will ensure that I keep my password secure and try not to leave my machine 'logged on'.
- 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 allow unauthorised individuals to access email / Internet / intranet or network.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (This is currently:lgflmail.org)
- I will only use the approved school email, school Learning Platform (VLE) 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 e-Safety Co-ordinator (David Petty), ICT leader (Anna Fisher) and the Network Manager (Ben Parker).
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will only connect a Tidemill computer, laptop or other device (including school issued encrypted USB flash drive), to the network / Internet and will ensure it has up-to-date anti-virus software.
- 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.
- I will not take school cameras home and will not store images of pupils outside of school (including on teacher laptops or teacher iPads).
- I will use the school's Learning Platform (VLE) in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create (or actively contribute to) are set to the highest security settings are not confused with my professional role.
- I understand that as a professional, I must not use a personal mobile, personal email or social networking sites to communicate with pupils or parents without permission from the head teacher.
- I agree and accept that any computer, laptop or iPad loaned to me by the school, is provided to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- I will access school resources remotely (such as from home) only through the school approved methods (RAV3) and follow e-security protocols to access and interact with those materials.
- If there is an essential reason to transport confidential data from one location to the other without using RAV3, I will liaise with the head teacher to gain permission to use an encrypted memory stick.
- 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 alert the school's named child protection officer / relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I will not connect to the school Wi-Fi or school email with personal devices, including personal phones, iPads and laptops.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school (David Petty).
- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): Staff agreement form

User Signature

I agree to abide by all the points above.

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

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

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

Full Name ..... (printed)

Job title .....

School .....

Authorised Signature (Head Teacher (primary) / Head/Deputy Head / Assistant Head / Phase Leader

I approve this user to be set-up.

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

Full Name ..... (printed)