Great Totham Primary School
Computing Policy

Context

Computing encompasses the use of digital devices of any description, Internet technologies and electronic communications such as mobile phones, digital cameras and wireless technology. This policy recognises the need to educate **all** members of the school community about the benefits and risks of using digital technology and provides safeguards and guidance for all users, to enable them to control their online experiences. This is explained as 'E-safety'.

Great Totham Primary School's Computing Policy will operate in conjunction with other policies and guidance including those for Pupil Behaviour, Bullying, Learning, Teaching for Learning, Staff code of conduct and behaviour, Complaints, Safeguarding and Child Protection.

Intranet and school to school systems

The school's intranet and school-to-school systems are in place to support the management and administration of digital files held by the school. Staff have a responsibility to use the school's intranet and school-to-school systems appropriately, in accordance with the Staff Code of Conduct, General Data Protection regulations (GDPR) and school data protection policy ensuring that all files are kept safe and secure. The use of personal external storage devices such as USB memory sticks are not permitted due to the risk of virus transfer and loss of data; all relevant staff members are provided with an encrypted USB device, to be used for professional purposes only. Staff are not permitted to upload files to the intranet from unknown sources as damage to the system is possible. Any suspicion of virus (or similar) being transferred to the system must be reported immediately to the computing leader or other senior member of staff.

E-safety

Good Habits

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

- Responsible digital technology use by all members of the school community.
- Guidance for safe and appropriate use of digital technologies shared explicitly with all pupils and staff, one such method being via this policy.
- Sound implementation of e-safety policy in both administration and curriculum use, including secure school network design and use.
- Safe and secure broadband from Schools Broadband, TalkStraight, including the effective management of content filtering.
- Sharing good practice with parents regularly and in specific situations.
- Refreshing and revisiting knowledge of apps and new risks and behaviours.

Internet use at Great Totham

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement and progress and to support the professional work of staff.
- Pupils will have access to the Internet both inside and outside of school and will need to learn how to evaluate Internet information and to take care of their own safety and security, beyond the security of the school's Internet filter.
- Staff will have access to the Internet both inside and outside of school and will need evaluate the appropriateness, safety and security of all websites/web pages used including when using them with the children.
- Staff must take responsibility for their own safety and security.

Authorised Internet Access

- At Great Totham all staff and governors read and agree to our 'Acceptable Use Agreement' and consult and follow the Staff Code of Conduct, before using any school digital device.
- Pupils and parents will be asked to sign and return an age appropriate (KS1 and KS2) form for pupil access to the Internet.

Safe Use of the Internet

- If staff (or pupils using the school network under their supervision) discover unsuitable sites, the URL (address), time accessed and content must be reported to their line manager or a senior leader who will report the issue to the Internet Service Provider (ISP).
- The school will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- Pupils will be taught how to report e-safety concerns through universally accessible means (e.g. CEOP report button).

Filtering

- The school will work in partnership with the Internet Service Provider to ensure filtering systems are as effective as possible.
- Staff and pupils are given different levels of filtering protection.

Messaging, E-Mail & Social Networking

- Staff should refer to section 7 of the Staff Code of Conduct.

We recognise that members of the school community have access to the Internet and messaging/social networking sites outside of school and that e-mail is often an essential means of communication. We make the following notes on the use of social networking and messaging applications;

- At school, pupils may only use approved messaging systems approved by the Head teacher and IT Leader. Currently, this is restricted to Google Classroom communication between teacher and pupil only although additions will be made on approval by the IT Leader or Head teacher.
- Filtering systems managed by the Internet Service Provider, prevent children being able to access social networking and media sites on school devices.
- Parents will be educated on how social networking can exploit the vulnerability of an individual, especially children, through regular e-safety events and specific support in individual or group situations.
- Pupils will be taught that they must not reveal personal details of themselves or others in digital communication, arrange to meet anyone without specific permission or give out information that identifies them or their location.
- Pupils must immediately inform an adult/member of staff if they receive an offensive message or a message that concerns them in any way.
- No member of the school community is to forward chain letters.
- In order to prepare pupils for life in the digital world they should be taught about security and encouraged to set strong passwords, deny access to unknown individuals and instructed how to block unwanted communications, including knowledge of the CEOP report button.
- Pupils will be taught about the risks of messages, images and content becoming available in the public domain.

Published Content and the School Website

- The contact details on the school web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content of school web site pages is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will never be associated with a child's name. Parents will give consent for the use of photographs and work displayed on the website or media.

Digital System Security

- School computing systems, capacity and security will be reviewed regularly by the head teacher, computing leader, computing technician and governors.
- Virus protection will be enabled and updated regularly.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.

Assessing Risks

- The school takes 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 school technology. Neither the school nor the Internet Service Provider can accept liability for the material accessed, or any consequences of Internet access.
- The school monitors children's understanding of e-safety to ensure the policy and curriculum are having impact.

Preparing Pupils for Life Outside School

- At Great Totham we recognise the different levels of risk associated with in school and out of school digital technology use. As part of the e-safety curriculum we will prepare pupils for the risks they face both in and out of school including developing uses of technology such as sexting, flaming (an unpleasant verbal exchange online), grooming, video sharing and other social media risks at an age appropriate level.
- In accordance with the Prevent Duty (June 2015) and with reference to the school's Child Protection and Safeguarding policies all staff are aware of the risks of radicalisation and teach pupils, at an age appropriate level, how to interact with others online and how to evaluate appropriateness. All staff complete safeguarding, E-safety and Prevent training annually.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure. Please see the complaints policy.

Communication of Policy

Pupils

- Children will agree to the relevant e-safety rules for their key stage. Pupils are reminded of these rules at the beginning of, and throughout, every year. New entries to the school will agree to the relevant e-safety rules for the key stage.

- Pupils will be informed that Internet use will be monitored.
- A copy of the e-safety rules (SMART rules) are sent home and displayed in the classroom and computing suite.

Staff

- All staff will sign an acceptable use agreement entitling them to use digital devices in the school environment.
- All staff will be given the school Computing Policy and its importance explained.
- All staff will be given relevant e-safety awareness training from a suitably trained member of staff.
- The e-safety curriculum will be shared with staff and key messages for each year group explicitly outlined. Advice for resources to support the curriculum can be requested from the computing curriculum leader or IT Leader. A number of government backed resources are freely available online.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to appropriate E-safety resources and be offered a copy of the e-safety rules for each child's key stage. They will be invited to regular e-safety awareness presentation where they have the opportunity to ask questions.
- Parents are offered computing support via the IT Leader, Mrs Liz Lawrence mrs.lawrence@greattotham.essex.sch.uk.
- Specific e-safety concerns will be raised by a suitable member of staff in individual cases.

Monitoring and review

The impact of this policy upon the quality of teaching and children's learning will be monitored and evaluated by the Computing Curriculum Leader. The Computing Curriculum Leader is responsible for reporting these findings to the Curriculum & Standards Committee.

This policy will be discussed annually with staff.

The Curriculum & Standards Committee will formally review this policy every two years.

Agreed by Curriculum & Standards Committee March 2015

Review Date:	Chair of the Committee signed:
March 2017	**Review**
March 2019	**Review** Minor amendments including GDPR
March 2021	Minor changes made to reflect computing developments

E-Safety Incident Guidance – Appendix A

E-Safety Rules (Pupils – Foundation and KS1) – Appendix B

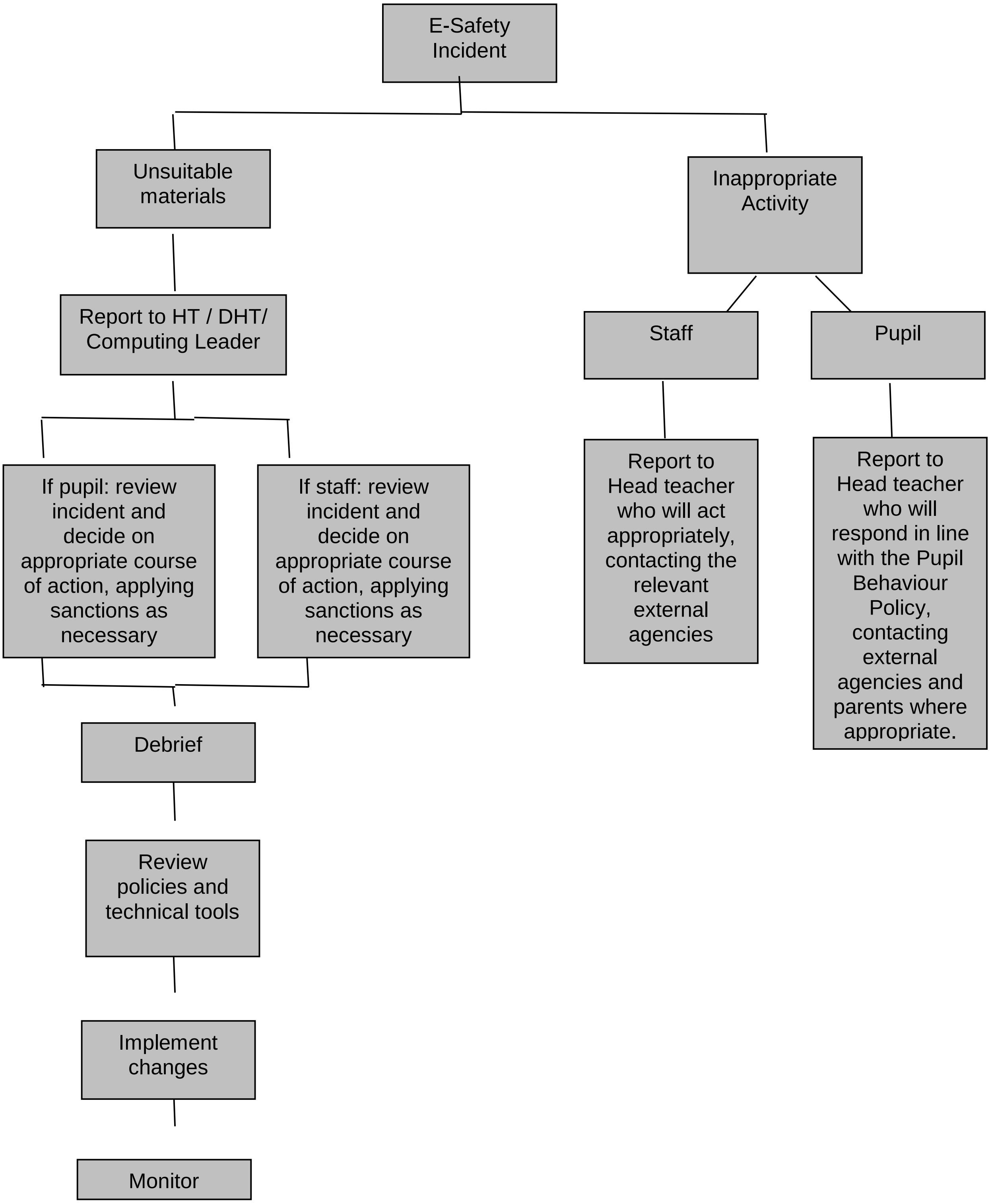
E-Safety Rules (Pupils – KS2) – Appendix C

Letter to parents – Appendix D

Staff Acceptable Use Policy – Appendix E

Appendix A

Flowchart for responding to e-safety incidents in school


E-Safety Incident
Unsuitable materials
Inappropriate Activity
Report to HT / DHT/ Computing Leader
Staff
Pupil
If pupil: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Report to Head teacher who will act appropriately, contacting the relevant external agencies
Report to Head teacher who will respond in line with the Pupil Behaviour Policy, contacting external agencies and parents where appropriate.
Debrief
Review policies and technical tools
Implement changes
Monitor

(Adapted from Becta – E-safety 2005)

Appendix D

Dear Parents,

As part of the computing curriculum, which aims to ensure that your child becomes a competent and active participant in our digital world, we require them to have access to the Internet. Our Internet services are filtered by Schools Broadband, Talkstraight who ensure that unsuitable websites are unavailable.
E-safety is an integral part of the computing curriculum and we will, at an age appropriate level, prepare your child for the dangers they will face on the Internet and the risks and benefits involved in its use.
Please read and discuss the attached agreement with your child and then **return the signed copy** (both parent and child to sign) to the school office. Attached below are e-safety rules that are used in school and will be useful for you to use with your child at home. By attending our e-safety parent talks, or using any of the online resources below~~,~~ you can learn more about helping your child to stay safe online.
E-safety agreements will be sent home at the beginning of every year to remind everyone of their responsibilities with online safety.

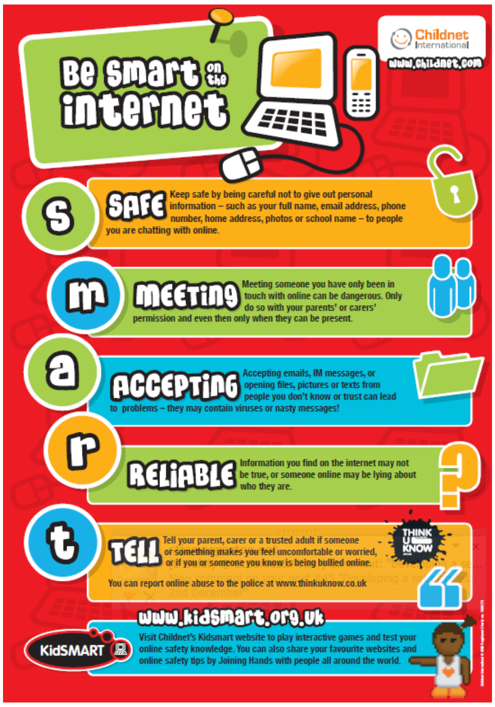
<u>The most important E-safety message for parents;</u>

‘Be the one your child can go to if they need help (not the one who will take their devices away without listening to them first)’.

Should you have any questions please do not hesitate to contact the office to make an appointment to see me.

Yours sincerely,

Liz Lawrence
IT Leader



SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Appendix E

Staff Acceptable Use Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct.
Staff should consult the school's computing policy for further information and clarification and MUST be familiar with the school's Staff Code of Conduct –in particular Section 7.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I will ensure my personal use of social media is compatible with my professional role and is in line with the guidelines in the Staff Code of Conduct and never brings the school, the staff or pupils into disrepute.
- I understand that school information systems may be used for incidental personal use (please see Staff Code of Conduct Section 7.1).
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that, in line with GDPR and the school's data protection procedures, personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Data taken off site must be appropriately risk assessed and any loss of data reported to the Head Teacher or Data Protection officer immediately.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Designated Child Protection Coordinator. This includes any concerns regarding potential radicalisation of any individual in accordance with the guidance set out in the Prevent Duty, June 2015.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to themselves, to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Staff Acceptable Use Code of Conduct.

Signed: ……………………………………………… Printed: ……………….……………………………. Date: ……………….……….

Visitor Acceptable Use Code of Conduct

To ensure that visitors are fully aware of their responsibilities when using technology in school, they are asked to read this code of conduct.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner (the school).
- I will ensure that my information systems use will always respect the role I have within school.
- I will ensure my personal use of social media is compatible with my role in school and never brings the school, the staff or pupils into disrepute.
- I understand that the school may monitor my information systems and Internet use within school to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Designated Child Protection Coordinator. This includes any concerns regarding potential radicalisation of any individual in accordance with the guidance set out in the Prevent Duty, June 2015.
- I will ensure that any electronic communications with pupils are compatible with my role in school.
- I will promote e-safety with pupils and will help them to develop a responsible attitude to themselves, to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.