Computing Policy

INCLUDING E-SAFETY AND CODE OF CONDUCT

Reviewed and Approved by: Governing Body on 6th February 2019

Review date: Autumn 2022
COMPUTING POLICY
At Chalkwell Hall Infant School we seek to develop children’s understanding and appreciation of Computing and the way it impacts on our lives. We believe it is essential to provide opportunities in all National Curriculum subject areas for children to develop their computing capability and to use it to support their learning. Computing makes education accessible to all, irrespective of learning styles and individual needs. At Chalkwell Hall Infants School Computing education is provided in a safe, happy and disciplined environment to stimulate and challenge both pupils and staff.

Aims & Objectives
• To encourage children to develop positive attitudes to Computing and to understand its importance and relevance to today’s world.
• To enable children to acquire a broad range of Computing capabilities and to be confident about using a range of hardware and software.
• To enable children to develop Computing as a tool for learning and investigation in all subject areas.
• To use Computing to encourage children to work co-operatively, taking responsibility collectively.
• To use Computing to develop independent ways of working which encourage children to take responsibility for their own actions.
• To set Computing tasks which require flexibility of mind and open mindedness in problem solving.
• To provide a balanced range of progressively more difficult tasks which will develop children’s understanding in algorithms, programming, using technology safely, collect and present data and understand different computer networks.
• To instruct children in the use of a variety of Computing equipment.
• To ensure a balance of Computing activities are carried out in a range of contexts.
• To provide opportunities for children to explore the use of technology.
• To set aside time for discussion of children’s experience of using Computing, both in and out of the classroom.
• To educate children in e-safety to ensure that they are safe when using the internet and know how to report possible dangers.

Teaching & Learning – KS1
Teaching and Learning will be based around the scheme provided ‘Purple Mash’ which is part of the 2Simple online software. KS1 will plan and teach using this progressive scheme to ensure a broad and progressive curriculum. Teachers are able to adapt the plans to
cater to the needs of their class to ensuring that the National Curriculum objectives are covered.

Teaching and learning will have an emphasis on whole class activities. New knowledge or skills will be taught by the teacher to the class and these will be reinforced by the class activities using laptops.

There will be lessons where the teacher is repeating a skill in order for the children to understand it or to further their knowledge.

Teaching and learning in class will include the use of iPads. Children will be taught how to use apps that enhance their learning in Computing and across the curriculum.

**Foundation Stage**

The early learning goals are the key focus for Computing and these are incorporated in the long, medium and short term plans. Foundation Stage are able to access a scheme of work on Purple Mash via Mini Mash to develop basic skills in Computing. All children in Foundation Stage will receive whole class Computing teaching to develop their knowledge and understanding ready for KS1.

Foundation Stage will also have the opportunity to develop their use of iPads and use apps to support and enhance their learning.

**Planning**

The curriculum map and lesson plans provided by Purple Mash ensure coverage of the National Curriculum, progression of skills, knowledge and understanding of the use of Computing in all subject areas.

The use of iPads will be an integral part of our cross curricular teaching and will be planned for effectively. We will be using a range of apps including Tiny Tap, Explain Everything and Book Creator to enhance the children’s learning across Literacy and Mathematics as well as the foundation subjects.

Staff use the scheme of work and medium term planning to produce weekly plans. Differentiation by task, support or outcome will be used to support and extend all children. Short focused tasks will be used for children to consolidate or enrich skills learned.

**Special Educational Needs (SEN)**

For children with SEN, Computing can provide a means of reinforcing concepts and knowledge. Computing has excellent motivational potential for children experiencing learning difficulties or behavioural problems; for example using a word processing programme supports presentational skills and a spell check may help with spellings. SEN children may require greater access to Computing in short, frequent sessions. Where a child has a physical difficulty they may need specialist adapted computer equipment in order to experience the same opportunities.

**Equal Opportunities**
Each child, regardless of gender, ability, social and cultural background, has an equal entitlement to Computing capability. Activities may be adapted to ensure a full programme of Computing is provided for children with physical disability or impairment.

Assessment & Recording
Assessments are used to inform the planning for consolidation and development of Computing capability. Teachers make assessments against The National Curriculum objectives. Pupils should be involved in the assessments of their own attainments.

During a topic, the work completed will be stored on Purple Mash and is accessible by the Computing Leader and class teachers. The Computing leader will keep samples of pupils’ work from each year group in a portfolio.

Resources
Each classroom has access to iPads. FS and Year 1 have access to an iPad trolley, and Year 2 has access to the iPad trolley. The laptop trolley has 30 networked laptops. Each Year Group has access to a wide range of software as well as the Internet (via a broadband connection).

Each class has an interactive LED touchscreen which is used daily to enhance teaching and learning.

All other hardware and software can be found in the server room.

In addition to the computers there is a range of other Computing resources including a teacher iPad that is used to take photographs and videos. It is also used as a visualiser when connected to a PC via AirServer. The small hall has a laptop connected with full access to the network. The dining hall laptop is connected to a projector and sound with access to the server through a local staff login.

Monitoring & Review
The Computing leader and BBC Team are responsible for monitoring and evaluating the use of Computing in school, providing support, organising training and arranging whole school INSET when appropriate.

The Technician is responsible for monitoring the condition of Computing equipment in school and organising repair/replacements as and when it is necessary. The Computing team plan ahead to ensure the continuous updating of equipment and resources.

The Computing Technician is responsible for the budget. The Computing leader and BBC Team are responsible for reviewing and updating the Computing policy and the schemes of work. The leader monitors the teaching and learning within the subject area.

Whenever subject curriculum is reviewed, as part of staff or curriculum development, the use of Computing in that particular subject will be an integral part of the training/planning.

e-Safety
The Acceptable Use of the Internet and related Technologies

The Internet is an essential element in 21st century life for education, business and social interaction. Computing skills and knowledge are vital to access life-long learning and employment; indeed Computing is now seen as a functional, essential life skill along with English and Mathematics. The statutory curriculum requires pupils to learn how to locate, develop, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely and to develop a responsible and mature approach to accessing and interpreting information. The Internet can benefit the professional work of staff and enhances the school's management information and business administration systems.

Whole school approach to the safe use of Computing

Creating a safe Computing learning environment includes three main elements at this school:

- an effective range of technological tools;
- policies and procedures, with clear roles and responsibilities;
- a comprehensive e-Safety education programme for pupils, staff and parents.

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. At Chalkwell Hall Infants School we are committed to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of, and respond responsibly to, any risk.

In line with the Safeguarding and Child Protection Policy, including Appendix Three on Prevent, staff are aware of the need to identify potentially vulnerable children and to ‘Notice, Check and Share’ in order to take proportionate action. In the circumstances of e-safety this could incorporate conversations with parents regarding the need to monitor children’s online gaming interest to prevent inappropriate approaches from unknown individuals which could result in radicalisation.

School is currently rolling out Prevent training to all staff and will include this as part of the induction procedure for all new staff from now on. See Safeguarding and Child protection Policy Appendix 3, Prevent.

The computing, e-safety leaders and Designated Lead are trained by the Child Exploitation and Online Protection (CEOP) centre. This is recognised e-safety training and allows the member of staff to train all staff members at Chalkwell Hall Infants and provide parents with an e-safety workshop.

The technologies

New technologies are enhancing communication and the sharing of information. 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 on computers often using simple web cams and via mobile devices
• Blogs (an on-line interactive diary).
• Podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player).
• Social networking sites (Popular: Facebook and Twitter).
• Video broadcasting sites (Popular: YouTube)
• Chat Rooms
• Gaming Sites (Popular: Minecraft, Bin Weevils)
• Music download sites (Popular: iTunes)
• Mobile phones with camera and video functionality
• Smart phones with e-mail, web functionality and cut down ‘Office’ applications.

Although the majority of these are not used in school, staff and children should be aware of the risks involved when using these technologies.

Staff must only use their mobile phones at appropriate times of the day e.g. break times. During the school day their mobiles should be turned off or set to silent. Staff must not use personal mobile devices or cameras to take images of pupils or staff.

Pupils are not permitted to bring mobile phones or devices into school. Should there be a need for children to bring their devices in to school these should be turned off and handed to the class teacher/School Office to look after during the school day and be collected at 3.00pm. Mobile phones may not be used to take pictures of pupils and staff (use class cameras provided by the school). Any pupils who are seen with a mobile device during the school day will have their phone removed from them to be collected at the end of the school day.

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the headteacher, with the support of Governors, aims to embed safe practices into the culture of the school.

Our e-Safety leader ensures staff keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as Becta and CEOP. The school’s e-Safety leader ensures the Headteacher is updated as necessary.

All teachers are responsible for promoting and supporting safe behaviour’s in their classrooms and following school e-Safety procedures. Central to this is fostering a ‘No Blame’ culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the school’s Policy including:

• safe use of e-mail;
• safe use of internet including use of internet-based communication services, such as instant messaging and social networking. Staff are discouraged from being members of social networking sites. However, if staff are members they are reminded of the necessity of keeping their profiles secure and to avoid contact with
persons (particularly parents/pupils or ex-pupils) related to the school. Staff are reminded that any action or comment that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality will be classed as a instant dismissal matter;

- safe use of school network, equipment and data;
- safe use of digital images and digital technologies, such as digital cameras;
- publication of pupil information/photographs and use of website;
- eBullying/Cyberbullying procedures;
- their role in providing e-Safety education for pupils.

System Safety Measures
The school maintains broadband connectivity through E2Bn and so connects to the National Education Network. Additionally, the school has up-to-date anti-spyware, anti-spamware and antivirus software and approved firewall solutions installed on its network. To make sure rogue applications are not downloaded and hackers cannot gain access to the school’s equipment or into users’ files through Internet use, staff and pupils are not able to download executable files and software. Unfortunately, there is the potential for inappropriate material to get through any filtering system. Access to inappropriate sites can be blocked.

This school:

- works in partnership with E2Bn to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- ensures network health through appropriate anti-virus software and network set-up so staff and pupils cannot download executable files such as .exe/.com/.vbs etc.;
- utilises caching as part of the network set-up;
- ensures the systems administrator/network manager is up-to-date with services and policies;
- ensures the systems administrator/network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- never sends personal data over the Internet unless it is encrypted or otherwise secured.

Surfing the Web
Aimless surfing should never be allowed. Pupils should be taught to use the Internet in response to an articulated need e.g. a question arising from work in class. Search engines can be difficult to use effectively. The teacher will need to choose a topic with care, select the search engine and then discuss with pupils sensible search words, which should be tested beforehand.

Although Chalkwell Hall Infant School’s internet is provided by E2Bn who have strict filtering systems there are also child-friendly search engines available for added security e.g. http://yahooligans.yahoo.com/ http://www.askforkids.com/

Pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering and monitoring.
Therefore this school:

- fosters a ‘No Blame’ environment that encourages pupils to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or Computing leader;
- has a clear, progressive e-safety education programme throughout all Key Stages, built on LA/E2Bn/national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:
  1. to STOP and THINK before they CLICK;
  2. to expect a wider range of content, both in level and in audience, than is found in the school library or on TV;
  3. to discriminate between fact, fiction and opinion;
  4. to develop a range of strategies to validate and verify information before accepting its accuracy;
  5. to skim and scan information;
  6. to be aware that the author of a web site/page may have a particular bias or purpose and to develop skills to recognise what that may be;
  7. to know some search engines/web sites that are more likely to bring effective results;
  8. to know how to narrow down or refine a search;
  9. [for older pupils] to understand how search engines work;
  10. to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
  11. to understand ‘Netiquette’ behaviour when using an online environment such as a ‘chat’/discussion forum, i.e. no bad language, propositions, or other inappropriate behaviour;
  12. to not download any files – such as music files – without permission;
  13. to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos;
  14. to have strategies for dealing with receipt of inappropriate materials.
- ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright/intellectual property rights;
- makes training available annually to staff on the e-safety education programme;
- runs a rolling programme of advice, guidance and training for parents, including:
  - information in safety leaflets; in school newsletters; on the school web site;
  - demonstrations, practical sessions held at school;
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.
How will e-mail be managed?

E-mail is now an essential means of communication for staff in our school and increasingly for pupils and homes. Directed e-mail use in schools can bring significant educational benefits through increased ease of communication between students and staff, or within local and international school projects.

Schools in Southend have an appropriate educational, filtered Internet-based e-mail system through the East of England Broadband Network (E2Bn).

Technology:

Incoming and outgoing e-mail can be restricted to approved addresses and filtered for unsuitable content and viruses. This is the first line of defence.

By default any pupil accounts that are created are automatically assigned as ‘safemail’. This means that pupils can only exchange e-mails with pupils and teachers from the same school. If a teacher wants to open up a class or a year group for a certain amount of time or permanently, they can do this by removing the safemail restriction. This means that they would have a typical e-mail account that is able to send or receive e-mails with anyone.

All e-mails in the E2Bn system go through a filtering process for inappropriate language regardless of whether they are in safemail or not.

Where the school receives nuisance or bullying e-mails and the e-mail address of the sender is not obvious, it is possible to track the address using ‘e-mail’ tracking software.

Procedures

In the school context, e-mail should not be considered private and most schools, and indeed Councils and businesses, reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

The use of email in the school is limited to the use of accounts on the school domain within the school network as much as possible. Individual pupil e-mails such as janet.brown@school.la.sch.uk which allow pupils to send and receive messages to and from the wider world, need to be carefully allocated to appropriate situations.

Whole-class E2Bn e-mail addresses can be used in primary schools, to communicate outside the school community.

This school:
- does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example education@chalkwellhall-inf.southend.sch.uk for any communication with the wider public.
- will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- has accounts which are managed effectively, with up-to-date account details of users.
- introduces pupils to use e-mail as part of the Computing scheme of work.
- introduces the principles of e-mail through closed ‘simulation’ software.
- teaches about the safety and ‘netiquette’ of using e-mail i.e.:
o not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer;
o that an e-mail is a form of publishing where the message should be clear, short and concise;
o 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;
o they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
o to ‘Stop and Think Before They Click’ and not open attachments unless sure the source is safe;
o the sending of attachments should be limited;
o embedding adverts is not allowed;
o that they must immediately tell a teacher/responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
o not to respond to malicious or threatening messages,
o not to delete malicious or threatening e-mails, but to keep them as evidence of bullying;
o not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
o that forwarding ‘chain’ e-mail letters is not permitted.

Using Digital Images and Video Safely

Developing safe school web sites and Facebook.
The school website and our Facebook group are our online public-facing communication channel. The Facebook group is closed and membership to the group has to be approved by a senior member of staff. However, due to the large numbers of parents, grandparents and other family members that may wish to join the group, background checks will not be completed on all new members.

Many prospective and existing parents find it convenient to look at these for information and it is an effective way to share the school’s good practice and promote its work. A senior member of staff authorises the website and Facebook group content and checks suitability. Access rights are given to those with authority to upload content into sections of the website. This website portal functionality is included within the broadband package.

Use of still and moving images
The utmost care is taken when using photographs or video footage of pupils on the school website/Facebook. We do not use the first name and last name of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the school. Our rule is:
If the pupil is named, avoid using their photograph/video footage.
If the photograph/video is used, avoid naming the pupil.

If showcasing examples of pupil’s work we only use their first names, rather than their full names.

Images are always checked to ensure suitable dress is maintained.

In many cases, it is unlikely that the Data Protection Act will apply to the taking of images e.g. photographs taken for personal use, such as those taken by parents or grandparents at a school play or sports day. However, photographs taken for official school use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, pupils and students should be advised why they are being taken.

Parental permission is obtained before publishing any photographs, video footage etc. of pupils on the school website, or in a DVD. This ensures that parents are aware of the way the image of their child is representing the school.

Procedures:

Links to any external websites are thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience. Remember to keep checking the content of websites regularly as they can change substantially, even in a short space of time. We check all links regularly, not only to ensure that they are still active, but that the content remains suitable too.

Text written by pupils is always reviewed before publishing it on the school website

We ensure also that the school is not infringing copyright or intellectual property rights through any content published on the website, for example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

We monitor any guestbooks, noticeboards or blogs on the school’s website to ensure they do not contain personal details of staff or pupils.

When showcasing school-made digital video work, we ensure that pupils are not referred to by name on the video, and that pupils’ full names are not given in credits at the end of the film.

Digital images - photographs and video clips - can now readily be taken using mobile phones. Extreme abuse is the so called ‘happy slapping’ incidents sent to others or posted onto a website. It is therefore important to ensure that the risk of inappropriate use is minimised.

Staff should not use their personal phone or camera without permission e.g. for a school field trip. All photographs will be transferred to the school network and will not be stored at home or on memory sticks and used for any other purpose than school approved business.

Digital images/video of pupils are stored securely on the school network and old images deleted after a reasonable period, or when the pupils have left the school.

When saving pictures, ensure that the image file is appropriately named. Do not use pupils’ names in image file names or in <ALT> tag references when published on the web. [An ALT tag is the HTML text describing a displayed image, used mostly for reasons of accessibility, since the tag can be voiced by screen readers].
All staff and pupils should report any inappropriate use of images to the Computing team/SLT and understand the importance of safe practice. Staff and pupils also need to understand how to consider an external ‘audience’ when publishing or presenting work.

In this school:

• The Deputy Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained.
• Uploading of information is restricted to authorised personnel.
• The school web site complies with the school's guidelines for publications.
• Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.
• The point of contact on the website is the school address and telephone number. Home information or individual e-mail identities will not be published.
• Photographs published on the web do not have full names attached.
• We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school.
• Digital images/video of pupils are stored in the teachers' shared images folder on the network and images are deleted when children leave the school – unless an item is specifically kept for a key school publication.
• Pupils are taught about how images can be abused in their eSafety education programme.

How will infringements be handled?
Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the head teacher.

Students

Category A infringements:

• Use of non-educational sites during lessons
• Unauthorised use of email
• Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
• Use of unauthorised instant messaging/social networking sites.

Sanctions: referred to class teacher.

Category B infringements

• Continued use of non-educational sites during lessons after being warned
• Continued unauthorised use of email after being warned
• Continued unauthorised use of mobile phone (or other new technologies) after being warned
• Continued use of unauthorised instant messaging/chatrooms, social networking sites, NewsGroups
• Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc.
• Accidentally corrupting or destroying others’ data without notifying a member of staff of it
• Accidentally accessing offensive material and not logging off or notifying a member of staff of it.

Sanctions: referred to Class teacher, e-safety leader/removal of Internet access rights for a period/contact with parent.

Category C infringements
• Deliberately corrupting or destroying someone’s data, violating privacy of others
• Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
• Deliberately trying to access offensive or pornographic material
• Any purchasing or ordering of items over the Internet
• Transmission of commercial or advertising material

Sanctions: as category B and referred to Headteacher.

Other safeguarding actions
If inappropriate web material is accessed:
1. Ensure appropriate technical support filters the site.
2. Inform E2Bn.

Category D infringements
• Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
• Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
• Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
• Bringing the school name into disrepute.

Sanctions – Referred to Headteacher/Contact with parents/possible exclusion/removal of equipment/refer to Community Police Officer / LA e-safety officer.

Other safeguarding actions:
1. Secure and preserve any evidence.
2. Inform the sender’s e-mail service provider.

Staff
Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

Sanction - referred to line manager/Headteacher. Warning given.

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school/Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

Sanction - referred to line manager/Headteacher. Action taken.