ABBEY ROAD PRIMARY SCHOOL
Computing Policy
(Including E-Safety and Acceptable Use)

This policy should be read in conjunction with other policies including Anti-Bullying, Behaviour, PSHE, Child Protection, Data Protection and Freedom of Information policies.

Introduction

Computing is an integral part of the national curriculum and a key skill for everyday life. Computers, tablets, programmable robots, digital and video cameras are a few of the tools that can be used to acquire, organise, store, manipulate, interpret, communicate and present information. We recognise that pupils are entitled to quality hardware and software and a structured and progressive approach to the learning of the skills needed to enable them to use them effectively.

School Aims

- Provide a relevant, challenging and enjoyable computing curriculum for all pupils.
- Meet the requirements of the National Curriculum programmes of study for computing.
- Use computing as a tool to enhance learning throughout the curriculum.
- To respond to new developments in technology.
- To equip pupils with the confidence and capability to use computing throughout their later life.
- To enhance learning in other areas of the curriculum using computing.
- To develop the understanding of how to use technology safely and responsibly.

Early Years

It is important in the foundation stage to give children a broad, play-based experience of Computing in a range of contexts, including outdoor play. Computing is not just about computers. Early Year's learning environments should feature technology-related scenarios based on experience in the real world, such as in role-play. Children gain confidence, control and language skills through opportunities to explore using non-computer based resources such as metal detectors, controllable traffic lights and walkie-talkie sets. Recording devices can support children to develop their communication skills. This is particularly useful with children who have English as an additional language.

By the end of key stage 1, pupils should be taught to:

- Understand what algorithms are; how they are implemented as programs on digital devices and know that programs execute by following a sequence of instructions
- Write and test simple programs
- Use logical reasoning to predict the behaviour of simple programs
- Organise, store, manipulate and retrieve data in a range of digital formats
- Communicate safely and respectfully online, keeping personal information private, and recognise common uses of information technology beyond school.

By the end of key stage 2, pupils should be taught to:

- Design and write programs that accomplish specific goals, including controlling or simulating physical systems
- Solve problems by decomposing them into smaller parts
- Use sequence, selection, and repetition in programs; work with variables and various forms of input and output; generate appropriate inputs and predicted outputs to test programs
- Use logical reasoning to explain how a simple algorithm works and to detect and correct errors in algorithms and programs

- Understand computer networks, including the internet; how they can provide multiple services, such as the world-wide web; and the opportunities they offer for communication and collaboration
- Describe how internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely
- Select, use and combine a variety of software (including internet services) on a range of digital devices to accomplish given goals, including collecting, analysing, evaluating and presenting data and information.

Planning

At Abbey Road, the Computing curriculum is organised into three main strands which begin in Early Years and are taught through to Year 6:

Everyone Can Code

This area of Computing progresses children's understanding of computer science through the specific teaching of coding. Children learn computational thinking skills which will help develop their problem-solving skills and they also become programmers by learning cornerstone coding concepts, including the specific coding terminology. In EYFS and KS1 children use practical tools and toys as well as apps to explore computational thinking. As children move through the school, they will use Discovery Coding lessons online to develop their programming skills and understanding. In Year 6, this will develop further where children will be introduced to Swift coding language.

Everyone Can Create

We aim to prepare our young people to participate in a rapidly changing world in which work and other forms of activity are increasingly dependent on the use of technology. This area of Computing develops pupil's digital communication and creative skills of images, film and data handling. They learn to save and retrieve work, type and use touch screens or mice and research online. Most importantly though, they learn to present and evaluate their digital work for a particular audience and purpose.

Everyone Can Stay Safe

No child should feel unsafe when using technology, including being safe online. Children will know what online bullying and online safety is and how to manage problems if they arise. They will become capable of thinking critically about the information they find online and understand the ways in which it may be used. We will teach them how to make informed judgements of when technology should be used and how it can achieve maximum benefit to work and learning.

Assessment and record keeping

Computing progress will be assessed in line with the progression of skills for each of the three stands of the curriculum. These outline the content to be taught in all aspects of Computing. Teachers regularly assess capability through observations and assessment of completed work. Assessing computing work is an integral part of teaching and learning and central to good practice. Assessment is generally in the form of formative assessments, which are carried out during and following short, focused tasks and activities. They provide pupils and teaching staff with the opportunity to reflect on their learning in the context of the agreed success criteria. This feeds into planning for the next lesson or activity. Computing work can be saved within Microsoft Office 365.

Monitoring and evaluation

The subject leader is responsible for monitoring the standard of the children's work and the quality of teaching. The subject leader is also responsible for supporting colleagues in the teaching of computing, for being informed about current developments in the subject, and for providing a strategic lead and direction for the subject in the school.

Equal opportunities

We will ensure that all children are provided with the same learning opportunities whatever their social class, gender, culture, race, disability or learning difficulties. As a result, we hope to enable all children to develop positive attitudes towards others.

Security

Our IT partners (Atom IT) will be responsible for ensuring the schools infrastructure is secure and not open to misuse or malicious attack, regularly updating anti-virus software. They will also ensure that all aspects of the school's ICT systems are secure.

Use of technology will be in line with the school's 'Acceptable Use Policy' for both pupils and staff. Staff and children must sign a copy of the schools AUP (see appendices). For pupils, this will be called 'The Abbey Road Technology Promise' which makes clear the school's expectations around use of technology. These are also displayed within each classroom and also within Home/School Record Books.

Social Media

As a school we recognise that social media and networking are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs, using these for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks. The school will use a Twitter account as a means of communicating with the school community. This account will be governed by senior leaders.

Social media and staff

Staff should:

- Ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.
- Not accept current or ex-pupils as 'friends' on social media sites such as Facebook.
- Be strongly advised not to accept parents, ex-parents and governors as 'friends' on social media sites. We do understand that some staff members have friends within the local community and ask that these members of staff take extra precaution when posting online. Where staff do accept friendships, they must not engage in discussion regarding the school, whether expressing personal views/opinions or any confidential information.
- Ensure that if their communication is fully public (e.g. blogs/ *Twitter/ Instagram* etc), that they maintain professionalism at all times and remember that they are a representative of the school.
- Be aware that electronic texts can sometimes be misinterpreted or misconstrued so should endeavour to minimise the possibility of this happening.
- Not use social media to discuss confidential information or to discuss specific children.
- Check with the school IT providers (Atom IT) if they need advice on monitoring their online persona and checking their security settings.
- Alert the head teacher immediately if they become aware that there is information about them held on social networking sites that causes them personal concern.

This subject is further covered within our staff Code of Conduct in relation to safeguarding children.

E-Safety

At Abbey Road we take e-safety very seriously. Children have dedicated e-safety lessons each half term as outlined within the '*Everyone Can Stay Safe*' progression document for Computing. E-Safety is also part of our PSHE curriculum. Content will be reviewed regularly to ensure it remains up-to-date and reflects current needs. Children will be taught how to act online and how to minimise the risk when working on the Internet. Lessons will cover a range of topics:

- how to identify and manage personal information
- how to recognise online bullying and what to do about it
- how to consider our own and others' wellbeing

- to be aware of our digital footprint
- how to respect copyright

Our plans will provide children with an understanding of the expectations we have of them at a level appropriate to their age.

All children will be taught about the Acceptable Use Policy (AUP) and will sign a copy related to their age phase. This also forms part of the Home-School Agreement, which pupils and parents read and sign upon entry to school.

Staff will be provided with e-safety training to ensure they are well-informed in terms of possible risks to pupils and understand their role in terms of safeguarding children.

Roles and Responsibilities

Governors are responsible for the approval of this policy and reviewing its effectiveness.

The Headteacher is responsible for:

- ensuring that everyone in school – including staff, volunteers and pupils - knows how to stay safe, including on-line.
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- ensuring that staff receive suitable training and development to enable them to carry out their role.
- ensuring that e-safety issues that occur within school and outside of school are appropriately dealt with, liaising with the Local Authority Designated Officer (LADO) or police as appropriate.
- providing information to the Governing Body, as appropriate.

Lead Teacher for Computing and E-safety is responsible for:

- ensuring staff have an up-to-date awareness of e-safety matters.
- updating school e-safety policy and curriculum content, as appropriate.
- monitoring curriculum delivery and outcomes.
- liaising with the Headteacher to provide training and advice to staff.

Classroom staff are responsible for:

- maintaining an up-to-date awareness of e-safety matters and of school e-safety policy and practice.
- ensuring they have read and understood the appropriate ICT agreements.
- reporting any suspected misuse or problem to a member of SLT.
- ensuring digital communications with pupils are only on a professional level and carried out using official school systems.
- understanding that social media can play an important part in communication between the school and parents/carers; but knowing it must be used in an appropriate and safe way.
- informing the Headteacher before setting up a digital resource such as a student blog space.
- ensuring that appropriate steps are taken to make such platforms 'private' so that only people they approve can access it. The member of staff will then be responsible for the posts made on the site and for moderating the content from users/contributors.
- teaching agreed e-safety objectives, as outlined within the Computing and PSHE curriculum.
- ensuring that children understand and follow the school's 'Acceptable Use' policy.
- making sure that children are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that children understand school policy in relation to mobile phones on site.
- ensuring that internet use in lessons is pre-planned and children are guided to sites that are checked as suitable for their use.

Children (appropriate to age / stage of pupil):

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- 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.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's Computing/E-Safety Policy covers their actions outside of the school gates and at home.

Parents

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through communications and the website.

Designated Persons for Safeguarding should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet.

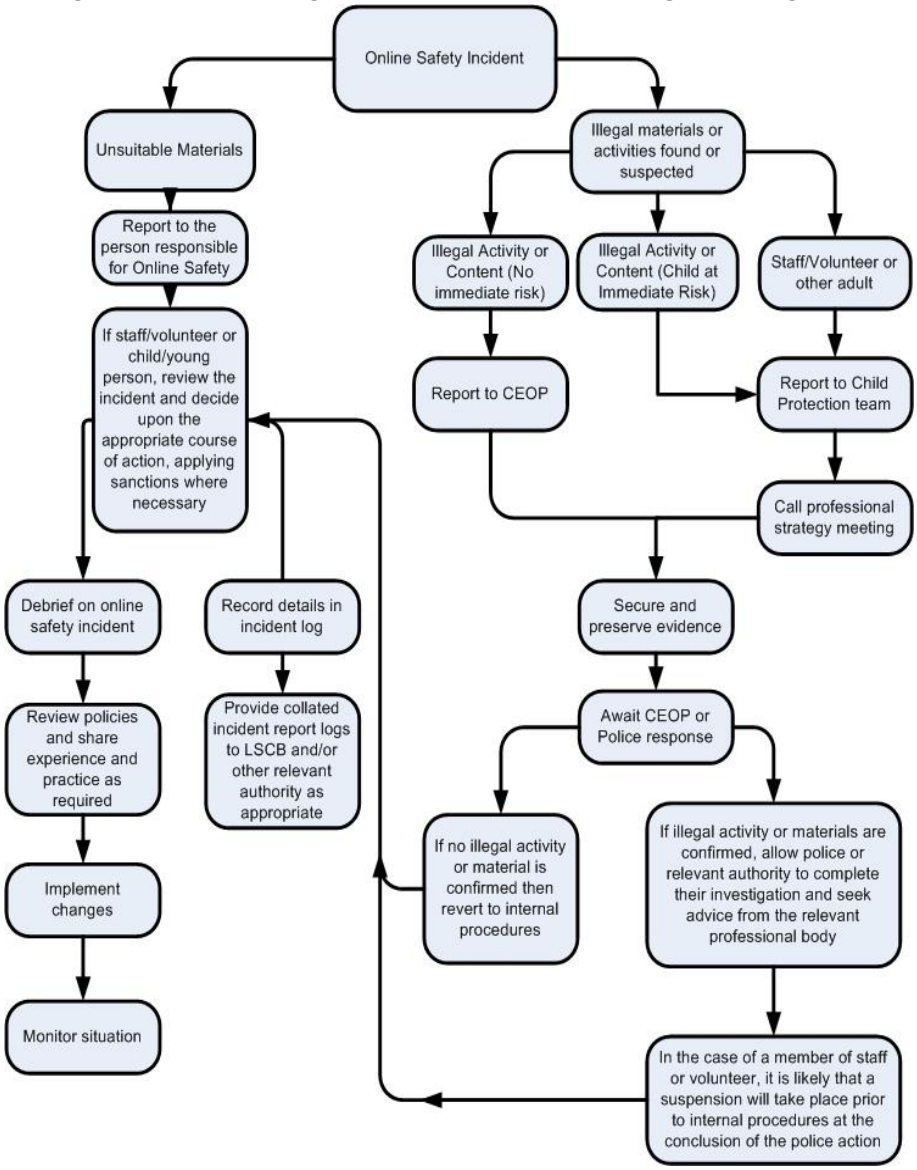
When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

Dealing with e-safety concerns

In the event of e-safety issues/concerns, school leadership will follow the attached flowchart, created by the Local Authority.

Responding to incidents of misuse – flow chart



Acceptable Usage Policy – Staff

This document has been written to ensure that staff use the ICT throughout the school appropriately. If they have any questions regarding this policy, they should direct them to Senior Management team or the ICT Coordinator. Staff should:

- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- In the event of the filtering system needing to be switch off for any reason, or for any user, this must be logged and carried out by a process that is agreed by Headteacher
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager
- Personal use of the school's ICT systems should be limited to what may be deemed reasonable. The services are provided predominantly for education purposes
- Neither staff nor students should install programmes or other software on workstations, portable devices or servers, without the prior express, written permission of the school's Network Manager
- The school's ICT infrastructure and individual workstations are protected by up to date virus software
- Personal data (as defined by the Data Protection Act) cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured by password or other means
- Where staff have email accounts and other Trust data on their phone or other mobile device they must ensure that the device is locked with a password.
- Use computers and equipment with care and ensure children do the same e.g. water bottles should stay away from machines
- Ensure that they have a sensible password
- Ensure that usernames and passwords are not shared with children or other staff
- Ensure that they log off when they have finished using a computer
- Try not to be wasteful, in particular when it comes to batteries, printer ink and paper
- Ensure that online dialogue (e.g. blog posts or emails) with other schools, parents or children remains professional at all times
- Ensure that online activity is related to their professional duty and that personal use should be kept to a minimum
- Ensure that they are not using the school's ICT for financial gain e.g. auction or betting sites
- Ensure that they have read and understood the ICT Policy
- Be aware that software or hardware should not be installed without prior consent of the ICT Coordinator or head teacher
- Where data of a personal nature such as school reports, IEPs, correspondence, photographs and assessment data is taken home on a school laptop or other storage device, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must therefore be taken to ensure its integrity and security. It should be removed from any portable device including, USB pens and memory cards, as soon as is practical. Where staff are using their own digital equipment such as cameras and mobile phones, extreme caution is advised to avoid misinterpretation by others. Files should be transferred to school equipment as soon as possible;
- Report any issues to the Senior Management team or ICT Coordinator as soon as possible
- Return any hardware or equipment if they are no longer employed by the school

Signed _____

Print _____

Date _____

The Abbey Road Technology Promise

When using technology in school we will:

- ✓ TAKE CARE – when carrying equipment.
- ✓ ASK - before going online.
- ✓ TELL - an adult if something goes wrong.
- ✓ THINK - before I click.

We understand that if we are not behaving correctly, we may not be allowed to use technology in school.

All of the children in ☐ agree to this.

Signed by the teacher: _____

The Abbey Road Technology Promise

When using technology in school I will:

- ✓ TAKE CARE – when carrying equipment in the classroom and around school.
- ✓ ASK – an adult before going online.
- ✓ SPEAK- kindly to others when sending e-mails and blogging.
- ✓ KEEP- my personal information private (such as password, full name, address and school name).
- ✓ TELL - an adult if something upsets me while I am online.
- ✓ THINK - before I click (especially when printing and deleting).

I understand that if I am not behaving correctly, I may not be allowed to use technology in school.

All of the children in class ☐ agree to this.

Signed (Teacher) _____