



Computing and E-Safety Policy

Author: Headteacher

Approval: Full Governing Body

Date: January 2026

Next Review: January 2027

Introduction

This policy outlines the teaching, organisation and management of computing (ICT) taught and learnt at Castle Primary School.

The significance of computing

As well as being an important curriculum requirement, the ability to use IT effectively is a vital life skill. We interpret the term 'Computing' to include the use of any equipment, which allows users to communicate or manipulate information electronically.

At Castle Primary School we endeavour to;

- use computing where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum
- use computing to help improve standards in all subjects across the curriculum
- develop the digital literacy and computer science skills of pupils through computing lessons and provide them with the chance to consolidate these in a cross-curricular context
- ensure pupils are challenged in their use of computing and are provided with exciting, creative ways in which to share their learning
- use tools available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation
- provide all staff with the training and support to ensure that they can, and have the confidence to, use computing to its full potential in all aspects of school life
- use computing as a form of communication with parents, pupils and the wider community
- make all users aware of the appropriate and safe use of computing.

We teach computing to develop:

- A positive attitude towards computing and an awareness of the fascination of and function of technology;
- Digital literacy and understanding of computer science;
- Appropriate uses of computing;
- independent learning;
- Motivation and self-esteem by exploring different ways to present their work;
- Collaborative and investigative skills, abilities and understanding;
- An appropriate use of computational language in order to express ideas confidently and clearly;
- The ability to adapt to the rapid technological changes taking place in society;
- Provide children with a variety of creative environments (blogging and animation);
- Use computing to support learners with special needs;
- An increased awareness of keeping safe while on the internet.

In learning computing pupils will:

- Use computing with purpose and enjoyment;
- Develop their computing skills;
- Become autonomous learners;
- Begin to evaluate the benefits of computing and its impact on society;

- Explore the full range of activities within the curriculum as fully as possible and help all pupils reach the highest possible standards of achievement;
- Celebrate success in the use of computing;
- Develop learners who are inquisitive to 'create';
- Understand what to do if they see something of an inappropriate nature;
- Understand what to share and what not to share online.

To assess pupils' progress in computing we:

- Gather evidence of what individual pupils know, understand and can do in computing by observing them at work, listening to and discussing with them, and evaluating any work they produce;
- Frequently discuss and mark work together to ensure pupils have a clear understanding of how their computing knowledge is progressing;
- Report annually to parents on how well the pupil has achieved;
- Hold pupil conferencing to ensure children understand how to keep safe when using computing.

In our curriculum computing is taught:

Computing is a powerful tool, which can be used to enhance teaching and learning across the curriculum, challenging the most able while supporting those with learning difficulties. Pupils will be taught and given opportunities to consolidate skills through highly motivated cross-curricular activities. This will be achieved as follows:

- Computing is incorporated in the planning of each subject scheme of work.
- When planning lessons involving the use of computing, teachers identify activities in which the emphasis is on both the development of computing skills and the subject being supported.
- The teachers will also be following a computing scheme of work which runs through the school, from the National Curriculum requirements, ensuring the children's computing skills are developed year on year.

Roles and Responsibilities - Senior Management Team

The head teacher and other members of the senior leadership team are responsible for monitoring the teaching of computing throughout the school. The senior leadership team should decide on the provision and allocation of resources throughout the school in accordance to the school improvement plan, computing action plans and timescales. They should also ensure that the computing coordinator and teachers are following their roles as listed below and in accordance to job specifications and performance management targets.

Roles and Responsibilities - Computing Coordinator

The Computing Coordinator will oversee planning in all year groups throughout the school and be responsible for raising standards in computing. They will also be responsible for informing staff of new developments and initiatives and providing training where appropriate. The computing Coordinator is responsible for overseeing the assessment of computing across the school and providing opportunities to moderate computing ability. They are responsible for keeping the hardware inventory up-to-date and ensuring the school has the appropriate number, and level, of software licenses for all software within the school. The computing Coordinator is responsible for managing equipment and providing guidance for future purchasing

and for ensuring tools and procedures are sustainable. The computing Coordinator is to review the effectiveness and value-for-money for any subscriptions such as Seesaw.

The computing coordinator will take a day to day responsibility for e-safety. They will:

- Take a leading role in establishing and reviewing the school e-safety policies / documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Report regularly to Senior Leadership Team
- Provide training and advice for staff and parents

Roles and Responsibilities - Teachers

Other subject leaders and classroom teachers should be aware that it is their responsibility to plan and teach computing and to use computing within their class. This will be in accordance to the schemes of work provided by the computing Coordinator. They will also assist in the monitoring and recording of pupil progress in computing. Teachers have an up to date awareness of e-safety matters. They should also respond to, and report, any e-safety or cyber bullying issues that they encounter within or out of school in accordance with e-safety procedures as listed below. Whilst checking of personal sites on school equipment, e.g. email, is permitted during non-contact times, staff should be aware that this should only happen for a brief time and that they should be extra vigilant and ensure they are logged off appropriately. Staff should follow, and agree to, the Acceptable Usage Policy (Hampshire County Council AUP). This includes vigilance towards their online behaviour outside of school.

The use of mobile phones and other handheld devices is permitted during break times and outside of school hours. Phones should be put on silent mode during lessons, staff meetings and training.

Roles and Responsibilities - Governors and visitors

School governors should abide by the guidelines set out for staff and ensure that if they do use the computers and equipment within school that they are doing so safely. If either a visitor or governor wishes to have an account to logon to the school network, they should speak to a member of the senior leadership team.

Roles and Responsibilities - The School

As a school we will endeavour to ensure that parents and pupils are fully aware of ways in which the internet and computing can be used productively and safely. We will always ensure that we provide children with the opportunities to excel and achieve when using computing and will ensure our curriculum is challenging and relevant. Before launching any system or initiative, we will make sure that the children's safety is at the forefront of our thoughts and we will keep parents informed as necessary through newsletters and parents' events. A range of e-safety websites will be made available on the school website.

The school will provide the following e-safety training:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The computing co-ordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The computing Coordinator will provide advice / guidance / training to individuals as required.

Roles and Responsibilities - Pupils

Pupils should follow the guidelines laid out in the AUP. They should ensure that they use the computers and equipment appropriately at all times.

It is expected that children will follow the school's behaviour policy when working online. They are also expected to adhere to the school's Anti-bullying policy. If the children fail to do so, then the procedures outlined in these policies will come into force.

Roles and Responsibilities - Parents

Parents should stay vigilant to the websites and content that their children are accessing. They should also try to talk to their child about e-safety and the use of the internet. If they have any questions or concerns then they should speak to their child's teacher, the computing coordinator or the headteacher.

Use of Online Learning Platforms

On occasions, class teacher may decide to access and use online learning platforms such as Seesaw, Google Classroom and Microsoft Teams in case of isolations or enforced school closures. Before such cases children and parents will be given clear guidelines on our expectations of using such a platform. These include:

For parents:

- Ensure that your child keeps their microphone muted unless they are asked to unmute.
- Encourage your child to raise their hand (or use the hand icon) if they would like to speak or ask a question
- Please do not take or post photos from Teams.
- Nothing from Microsoft Teams should be uploaded to ANY social media site.
- Provide your child with a safe, appropriate place to work.
- Ensure your child wears suitable clothing.
- Make sure the camera angle is straight ahead.
- Please be mindful of language being used whilst your child is unmuted.
- Ensure you stay in the room with your child while the call is taking place.

For children:

- Join every call with your camera on and microphone muted.
- Keep you microphone muted unless you are asked to unmute yourself.
- Raise your hand, or use the hand icon on Teams, if you would like to speak.
- Make sure your adult is in the room with you during the Teams call.
- Make sure you are dressed appropriately.

- Ensure that there isn't anything in the background that you wouldn't want your class or teachers seeing.
- Make sure you pay close attention to the group and ensure you're not doing anything else e.g, playing games.
- Do not leave the view of the camera during the call.
- Respond to your teachers/friends as you would if you were in the classroom.
- Do not take any images or video of the class.
- Remember if you wouldn't do it in your classroom, don't do it in your virtual classroom.
- Do not post anything inappropriate or unrelated to your current learning online, as it may not be approved.

Class teachers will monitor the chat function throughout the call and ensure all chat is appropriate. Parents and children will also be made aware of the expectations for work to be completed, when this is to be submitted and how it will be marked. Any live lessons or Teams meet ups will be recorded.

Technical support

Staff are encouraged to resolve basic problems themselves. If there are any problems with the Software or hardware it must be reported to Drift IT or computing Co-ordinator. Where the problem cannot be resolved in school, the computing Co-ordinator will liaise with Drift IT services to resolve the problem.

Provision for Special Educational Needs

Pupils with Special Educational Needs can benefit from using computing as it enhances access to the curriculum, and this in turn encourages motivation and the development of skills. Computing resources in the school will reflect the needs of all our students and the computing Subject Leader will work with class teachers and the Special Educational Needs Co-ordinator who will work with outside agencies and advise staff to develop a portfolio of computing resources to support the needs of specific children in the school.

Internet

Castle Primary School actively encourages the use of the Internet to develop searching, questioning, interpreting, evaluating and sharing skills through a cross-curricular approach. We aim to introduce the Internet to every child in such a way that it contributes to effective teaching and learning.

Access to the Internet will be limited to those periods when the pupils are being closely observed by a member of staff to ensure issues of:

- safety
- security
- meaningful use

In addition, each child has a log-in which is known to staff members and the internet has a filtered system in place run by Hampshire County Council.

If, however, any pupil should encounter any offensive material accidentally, they are expected to report it immediately to a teacher. The teacher should then inform the computing Co-ordinator as to the address of the inappropriate site, as well as

corresponding links. The computing Co-ordinator will then inform the Internet Service Provider (ISP) and add the website's information to the filtered system.

Computing equipment is not to be used during break, lunch times or after school unless a member of staff is present.

E-Safety Guidelines

At Castle we take e-safety very seriously. We will ensure that it is taught often throughout the children's computing and PSHE sessions and in key stage assemblies as necessary. We will also provide children with dedicated e-safety lessons per term. All e-safety resources will be available on the school website for parents to view. These will be reviewed regularly to ensure that they are up-to-date and reflect current needs. Children will be taught how to act online and how to minimise the risk when working on the internet. Pupils will also be taught about managing passwords, respecting copyright and other elements of this policy that are relevant to them.

Our plans will provide children with an understanding of the expectations we have of them at a level appropriate to their age. We will also have an annual e-safety focussed parent meeting and will provide regular updates via our website and newsletters as appropriate.

All children will be taught about the Acceptable Use Policy and will sign a copy related to their age phase. These will be stored by the computing Coordinator. All staff will also complete an AUP. Useful computing rules will also be posted in the computing suite and on the storage facilities for mobile devices to ensure they are seen by children and visitors.

If a teacher suspects an e-safety issue within school they should make notes related to the incident in accordance to anti-bullying and behaviour policies. This should then be reported to the computing Coordinator and head teacher and recorded as appropriate.

Flexible Web Filtering

This is part of the HPSN2 service and will be used to decide which websites can and cannot be accessed from our school site. The computing Coordinator and SLT will consider all applications for website accessibility. A search engine enabling a 'safe search' will be the standard search engine throughout the school.

Equipment, Hardware and Software

Hardware should not be installed without the permission of the head teacher and/or computing coordinator. If staff use memory sticks then the school's antivirus software will scan these. Staff should be vigilant to reduce the risks of virus infection as stated in the AUP. Any data storage devices (memory sticks or external hard drives) should be password protected where sensitive information is stored.

The installation of software unauthorised by the school, whether licensed or not, is forbidden. If you are unsure, please speak to the head teacher and/or the ICT Coordinator for advice. The school reserves the right to examine or delete any files that are held on its system.

Tablets

The upkeep and updating of the iPads and tablets will be the computing coordinators responsibility. Staff will not have access to add any apps to the devices, if they have an app they wish to use, they will ask the computing coordinator to add it to the system. Apps will not be added that are not age appropriate. The use of apps will be monitored by the computing coordinator and any unused apps will be removed to avoid wasting memory. It is the teacher's responsibility to inform their class of appropriate use for the tablets and to ensure they are put away correctly. It is their responsibility to check that children are using the appropriate apps to the lesson and to delete any images that have been taken using the camera after their use. Dropbox will be used to temporarily store files so that they can be added to the school's system and then files will be removed from Dropbox.

The computing coordinator will monitor the use of the tablets annually and provide training where necessary to ensure their use throughout the school.

Copyright and Intellectual Property Right (IPR)

Copyright of materials should be respected. This includes when downloading material and/or copying from printed materials. Staff should not remove logos or trademarks unless the terms of the website allow it.

Staff should check permission rights before using materials, particularly images, from the internet.

Passwords – Linked to 360Safe Password Guidelines

Staff should make sure that any passwords they use are strong and contain a mixture of some of the following; upper- and lower-case letters, numbers and punctuation. These should be changed regularly, especially if the user suspects others may know the password.

Personal Data

Staff should be aware that they should not transfer personal data such as reports, IEPs and contact information on to personal devices, unless encrypted. Staff will have access to data via the Hosted School Service from December 2012. When using a personal laptop or device containing student data, staff should be extra vigilant to not leave this device lying around or on display and ensure that it has been logged off.

Social Media - Linked to 360Safe Social Media Guidelines

As a school we fully recognise that social media and networking are playing an increasing role within every-day life and that many staff and FOCs members 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.

Staff should:

- Ensure that 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. This is to ensure any possible misinterpretation. We do understand that some staff members have friends within the local community and just ask that these members of staff take extra precaution when posting online

- Ensure that if their communication is fully public (e.g. blogs/Twitter), that they maintain their 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 these media to discuss confidential information or to discuss specific children
- Check with the computing Coordinator if they need advice on monitoring their online persona and checking their security settings

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge. As a school we will monitor the use of social networking and ensure it is part of our curriculum. We will also ensure that parents are fully aware of how to minimise the risk if their children are using these sites. As a school, we do reserve the right to contact sites such as Facebook and ask them to remove our children's accounts should any issues, such as cyber-bullying, occur.

Digital and Video Images - Linked to 360Safe Digital and Video Guidelines

As a school we will ensure that if we publish any photographs or videos of children online, we will comply with GDPR regulations by:

- Ensure that their parents or guardians have given us written permission
- Ensure that if we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure that they are not left out of situations unnecessarily
- Will not include a child's image and their name together without permission from the parents or guardians e.g. if the child has won an award
- Will ensure that children are in appropriate dress and we do not include images of children who are taking part in swimming activities
- Ask that if a parent, guardian or child wishes, they can request that a photograph is removed. This request can be made verbally or in writing to the child's teacher or to the computing Coordinator. We will endeavour to remove the photograph as soon as possible
- Will provide new parents with a photo or media permission letter upon their arrival into school
- Will ask parents or guardians to refrain from taking videos or digital images that contain other children without permission, and these are not to be shared online.



CASTLE PRIMARY E-SAFETY RULES EYFS

Acceptable Use Policy

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

I have discussed these rules with my child and they understand what is expected from them and know what to do when there is an issue.

Pupil Signature:

Name:

Parent Signature:



CASTLE PRIMARY E-SAFETY RULES KS1

Acceptable Use Policy

I agree that I will:

Using Computers

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I know that if I break the rules I might not be allowed to use a computer / tablet
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will treat everyone online with respect and use kind words

E-safety

- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I will not share any personal information about myself or others with anyone online
- I will not tell anyone my password

I have discussed these rules with my child and they understand what is expected from them and know what to do when there is an issue.

Pupil Name:

Parent Signature:



CASTLE PRIMARY E-SAFETY RULES KS2

Acceptable Use Policy

I agree that I will:

Using Computers

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I know that if I break the rules I might not be allowed to use a computer / tablet
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong

Using the Internet

- I will ask before using the internet and use it for a specific focus
- I will treat everyone online with respect and use kind words
- I will not open or download a file unless I know it is safe
- I know that not everything I read on the internet is true
- I know that most forms of social media such as Facebook have a 13+ age rating and I need my parents permission and advice before using them
- I know that anything I 'post' on the internet is permanent

E-safety

- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I will not share any personal information about myself or others with anyone online
- I will not tell anyone my password
- I will not share pictures or videos of myself or others with anyone online
- I will never meet in person anyone that I have met online

Pupil Name:

Parent Signature:



STAFF / VISITORS CODE OF CONDUCT FOR ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, iPads, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the headteacher.
- I understand that I may not use any social networking sites to communicate with children that are on roll at Castle Primary School. (Family members excepted)
- I understand that I may use the systems within Education City to communicate with children and that all such communications will be recorded.
- I understand that if I do use a social networking site I will not make any statements that could embarrass or compromise; myself, the pupils, other staff members, Castle Primary School or my employer.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator (Deputy Headteacher), the Designated Child Protection Coordinator or Headteacher.
- I will report any incidents where I witness non-compliance with this policy.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete 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 accept the Staff Code of Conduct for ICT.

Signed: Capitals: Date: