Computing Policy
including Online Safety

Approved: April 2025

To be reviewed: April 2026

Computing Policy

1. Raddlebarn Primary School

This policy should be read in conjunction with other school policies including the Acceptable Use Policy (AUP), Anti-Bullying, Behaviour, Child Protection and Safeguarding.

2. Introduction

This policy aims to cover the different elements that information communication technology (ICT) and computing can cover within our school. These guidelines have been drawn up to ensure that all stakeholders within the school are aware of what is expected of them and are able to stay safe when using the hardware and software we have in school. The equipment and resources within school are provided to enhance the learning of the pupils and to aid the staff in their delivery of the curriculum; this policy will enable these to go ahead. This policy will set out a framework for how Computing will be taught, assessed, and monitored throughout the school and should reflect the ethos and philosophy of our school.

3. Aims/Rationale

ICT and computing encompasses every part of modern life and it is important that our children are taught how to use these tools and more importantly, how to use them safely. We believe that it is important for children, staff and the wider school community to have the confidence and ability to use these tools to prepare them for an ever-changing and rapidly developing world.

To enable all our staff and pupils to be confident, competent independent users and learners of computing we aim:

• To use ICT where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum

• To use ICT to help improve standards in all subjects across the curriculum

• To develop the ICT competence and skills of pupils through Computing lessons and provide them with the chance to consolidate these in a cross-curricular context

• To ensure pupils are challenged in their use of ICT and are provided with exciting, creative ways in which to share their learning

• To use tools available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation

• To provide all staff with the training and support to ensure that they can, and have the confidence to use ICT to its full potential in all aspects of school life

• To ensure all pupils use existing, as well as new, technology safely and develop an understanding of the use, importance and limitations of the internet and other digital technologies including the need to avoid undesirable material.

• To use ICT as a form of communication with parents, pupils and the wider community

4. Curriculum

Our curriculum, based on the National Curriculum, ensures a balanced coverage of computer science, information technology and digital literacy. The teaching and learning of Computing facilitate progression across all key stages within these three strands and is based on children's prior knowledge, with the provision of challenges of new learning. Our broad and balanced curriculum for the teaching of Computing prepares pupils to use computational thinking and creativity – and helps them to understand the rapidly changing world. This curriculum helps to equip pupils with high level skills in using ICT, preparing them to apply these across the curriculum in their ongoing educational journey.

We use the Purple Mash scheme of work that is in line with the National Curriculum. The Purple Mash overview, support materials and lesson plans are available to ensure teachers are able to fulfil the computing curriculum. We have supplemented some modules in Y4, 5 and 6 from the Teach Computing Scheme of Work. This is to ensure that children are exposed to new and improved forms of software in order to prepare them for an ever increasing digital world. The Computing Coordinator will ensure that the plans provide coverage of what is expected, through the National Curriculum Programme of Study. The Computing Coordinator will also ensure that through teaching and learning children are challenged and are able to succeed.

The Purple Mash scheme is made up of a) curriculum focused activities, b) creative tools, c) programs and games- to support and inspire creative learning every day. It is a useful resource to establish a meaningful, productive cross-curricular link between the teaching of Computing and other subjects. Through the Computing curriculum, children complete a number of projects each year covering: programming, computational thinking, creativity, computer networks, communication and collaboration and productivity. Teachers can plan and deliver each aspect of the Computing curriculum, due to the clearly led overview and the scheme of work.

The Computing Coordinator will alert all teachers to the need to discuss and teach online safety. The school follows the Purple Mash framework for teaching online safety skills throughout the year. Educating pupils about the online risks that they may encounter is also done informally when opportunities arise. The school promotes 'Safer Internet Day' each year with the aim of raising awareness around online safety issues. We also have a half-termly E-Safety assembly which focusses on current themes.

This curriculum helps children to become responsible digital citizens who can live and use technology safely and respectfully, recognise acceptable/unacceptable behaviours and identify a range of ways to report concerns about content and contact.

5. Online Learning

As a school, we value the importance of providing opportunities for children to learn outside of school and we will provide these depending on the age of the child.

On our website, for children and adults at home we will:

- Provide links to approved generic websites suitable for the age phase (e.g. phonics)
- Provide links to approved websites suited to the current topic where appropriate
- Provide a 'Our Learning' page where children can find out more about what to expect during the year by following the 'Curriculum Overviews' link

6. Assessment

Computing will be assessed in a number of ways using formative and summative assessment. Formative assessment will happen during computing lessons and will be used to inform future planning and this is conducted by the teacher on an informal basis. At the end of each computing project, children should be encouraged to peer assess and evaluate their own progress and learning. Children will store their work on the network, Purple Mash display boards or on iPads. Children's files should be used as an evidence base of the progress they are making.

7. Equal Opportunities and Inclusion

We will ensure that all pupils are provided with opportunities to access the computing curriculum throughout the school. Where necessary, we will endeavour to make adaptations to the environment or provide software that will enable all learners to achieve.

8. Roles and Responsibilities – Computing Coordinator and ICT Technician

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 monitoring, assessment and overseeing computing across the school. The Computing Coordinator and a designated member of the Senior Leadership Team will be the school's Online Safety Coordinators. It is the role of the Online Safety Co-ordinators to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet so that they can inform staff, as safeguarding is everyone's responsibility.

The ICT technician will be responsible for keeping the hardware inventory up-to-date and ensuring the school has the appropriate number, and level, of software licences for all software within the school.

9. Roles and Responsibilities - Staff

Other subject leaders and classroom teachers should be aware that it is their responsibility to plan and teach computing and to use ICT within their class. This will be in accordance with the Purple Mash schemes of work provided by the Computing Coordinator. Teachers should also respond to, and report, any online safety or cyber bullying issues that they encounter on CPOMS (under e-safety) and then alert the Online Safety Coordinators and a DSL promptly or immediately if it is a safeguarding concern. Staff should be aware that all internet use is monitored. Staff should follow, and agree to, the Acceptable Usage Policy (AUP) and the Computing Policy including Online Safety.

10. 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 ICT can be used productively and safely. We will always ensure that we provide children with the opportunities to excel and achieve when using ICT 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 parent's events.

11. Roles and Responsibilities - Pupils

Pupils should follow the guidelines laid out in the AUP (Acceptable Usage Policy). 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. Online safety rules and guidelines will be displayed in the ICT suite and

discussed when technology is used within the classrooms/lessons by all staff. Pupils will be informed that all internet use in school is monitored.

12. Roles and Responsibilities - Parents

Parents should stay vigilant to the websites and content that their children are accessing. They should also talk to their child about online safety and the use of the internet - there are resources on the school website to aid this. Parents should take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies. Parents should also liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online. If they have any questions or concerns then they should speak to their child's teacher or the Computing Coordinator.

13. Equipment, Hardware and Software

Hardware should not be installed without the permission of the head teacher. Staff should use encrypted 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. The installation of software unauthorised by the head teacher, whether licensed or not, is forbidden. If you are unsure, please speak to the head teacher for advice. The school reserves the right to examine or delete any files that are held on its system.

14. Staff Laptops and iPads

All Laptops & iPads remain the property of school and must be returned when requested. They are open to scrutiny by the senior leadership team. Laptops belonging to the school must have updated antivirus software installed and be password protected. The security of school laptops and iPads is of prime importance due to their portable nature and them being susceptible to theft.

15. Pupil iPads

Staff are responsible for ensuring children take care when using the iPads. If an iPad is taken off site this must be with permission from a member of senior leadership and used only for educational purposes. Staff are not permitted to install any apps on iPads without permission from the head teacher. All iPads are numbered e.g BK2. Teachers are to record which iPad children use during a lesson. This is to be able to track history back to a specific child and a specific time.

16. Network

Staff will be issued with a username for the computer and a simple password. It is their responsibility to change their password in accordance with the password procedure below. Pupils in Reception will not be expected to log on to the network and this may be done for them. Children in Year 1 will be expected to use a generic class login and password. From Year 2 upwards, children will be issued with their own username and password to access the school network. These accounts will be created and monitored by the ICT Technician.

17. School Website

Staff may use images of children on the website if parents have given consent – this can be checked through the school office. Children will be referred to by their first names only and photographs that include pupils will be carefully selected. 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.

18. Padlet

Padlet is used at Raddlebarn Primary School as an online platform for children to post their family homework achievements. The Padlet gives pupils a wider audience for their learning through the school community and therefore purpose.

Padlet Rules

- Using the Padlet safely and sensibly is important as it can be accessed by all of the children at Raddlebarn.
- Children will ask their parents'/carers' permission before they post on the school's Padlet, including the posting of any names, photos and videos.
- All contributions to the Padlet will be monitored by a member of staff and inappropriate comments will be deleted.
- The Padlet is not a forum for discussion – it is a means to celebrate homework achievements. Questions on the Padlet page will not be answered.

Additionally, the following rules, if followed, will minimise any risks and will ensure that children will stay safe whilst posting:

- Never give away any personal information about your location or identity.
- Do not post pictures/videos of yourself without specific permission from your parent/carer.
- Do not use inappropriate language (including text language) in your posts.
- If you see anything that should not be on your screen, do tell your teacher and parents immediately.

In addition, it can also be used as a home learning platform for children to share their work with teachers in a safe, password protected environment.

19. Internet

The internet may be accessed by staff and by children throughout their hours in school. We ask as a school that staff are vigilant as to the sites children are accessing and children should not be using the internet unattended. The teaching of email and internet use will be covered within the computing curriculum and incorporated within online safety lessons, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the internet.

Internet use will support, extend and enhance learning:

- Pupils will be given clear objectives for internet use.
- Web content will be subject to age-appropriate filters.
- Internet use will be embedded in the curriculum.

Pupils will develop an understanding of the uses, importance and limitations of the internet:

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate information on the internet.
- Pupils will be taught how to report inappropriate web content and seek advice as needed.

The use of the internet to access inappropriate materials is prohibited. If users, especially children, do see an inappropriate website or image, they should minimise the page immediately and report the

site to their teacher who will then pass this on to the Online Safety Coordinators. The internet and filtering is provided by the local authority and the technician will run speed checks at regular intervals to monitor the connection speed. Inappropriate websites are filtered out by the local authority. The school will work with the ICT technician to ensure that appropriate filtering is always in place. Additional sites can be enabled by the technician and a record will also be kept of the sites enabled by school.

20. E-mail

All members of staff will be issued with a school email address and this is the email with which they should use for professional communication. Through Purple Mash, children will be issued with an email address for specific computing projects and this should be monitored by the class teacher and the Computing Coordinator. Pupil email accounts will only be enabled for intranet use through the Purple Mash software and used within the Raddlebarn School Community.

- Pupils will tell a member of staff if they receive inappropriate e-mail communications.
- Pupils will only use e-mail for approved activities.
- Pupils should be taught not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission

Staff should not communicate with parents about children directly through email. Should they receive an email, relating to a child, staff should contact the parent via telephone or face to face and explain that emails should come through the enquiry@radlbarn.bham.co.uk address but the best way to contact school staff is by phoning in, speaking to staff on the door or visiting the school office. Staff should take extra care to ensure that all communication remains professional. Users are responsible for all messages that are sent and due regard should be paid to the content of the emails to ensure it is not misconstrued. It is the user's responsibility to ensure they log off appropriately. If children receive an email that they believe to be inappropriate then they should forward it on to their teacher who will investigate.

21. Passwords

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. For sites where children have passwords, they will be provided with these by either their teacher or the Computing Coordinator.

22. School Liaison, Transfer and Transition

When a new child joins, it is the responsibility of the class teacher to inform the ICT technician of the child's name and year group. The ICT technician will then provide a network login. Once they have left our school, the child's account will be removed and their content will be archived.

23. Personal Data

Staff should be aware that they should not transfer personal data such as reports, children's support profiles and contact information on to personal devices but should use OneDrive. If data is downloaded to a personal device it should then be removed as soon as possible. When using a laptop or device containing student data, staff should be extra vigilant to not leave this device lying around or on display e.g. in a parked car.

24. Social Media

As a school we fully 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. Please see the Raddlebarn Staff Code of Conduct and Social Media Policy for more information.

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. This is to ensure any possible misinterpretation does not occur. We do understand that some staff members have friends within the local community (such as children's parents) and ask that these members of staff exercise their professional judgement and do not contact family members on social media if it would lead to a conflict of interest.
- Ensure that if their communication is fully public (e.g. blogs/Twitter), that they always maintain their professionalism 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.

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 ensure this features as part of our online safety 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. Pupils are aware of the impact of cyber-bullying and know how to seek help if they are affected by any form of online bullying.

25. Blogging

We will use blogging, on Purple Mash, where appropriate in the computing curriculum. We will follow guidance laid out in this document to ensure children are kept safe. No-one is able to post on the blog or write a comment without it being approved by a teacher to ensure that children are not subjected to any inappropriate comments.

26. Digital and Video Images

As a school we will ensure that if we publish any photographs or videos of children online, we:

- Will ensure that their parents or guardians have given us written permission
- Will ensure 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 first name together without permission from parents or guardians
- 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 permission letter as part of the admissions procedure.

- Will ask parents or guardians that are recording videos or taking digital images at public events e.g. school play or sports day, that they do not publish these online. Any images/recordings shared on social media should be reported to the Computing Coordinator as soon as possible.

27. Mobile Phones

Pupils are not permitted to have mobile phones or other personal handheld technology in school. Children in Year 6, who walk home alone, must hand in their phones to the office on arrival at school. Such items can be confiscated by school staff if they have reason to think that they are being used to compromise the wellbeing and safety of others (Education and Inspections Act 2006, Sections 90, 91 and 94).

In addition, with the exception of the school's Headteacher and Business Manager, staff should not have their phone with them around the children unless they have been given permission from the Headteacher and it is for a specific reason such as for a school trip as a means of contact.

28. Technical Support

Any issues must be logged with the ICT technician on the Every web portal. These will then be dealt with by the Technician or Computing Coordinator as appropriate. It is all members of staff's responsibility to log any issues or speak directly to the appropriate member of staff.