Read St. John's Computing Policy

'Sowing the Seeds of tomorrow; growing in the light of the Lord'

At Read St. John's we aim to unlock the potential for everyone to flourish whilst being rooted and grounded in God's love. We aim high, so together as one family, we can fly.

This policy outlines the intent, implementation and impact of the teaching and learning of computing at Read St. John's. It has been written by the subject leader and is reviewed by the headteacher and governors. The subject is led by the subject leader and staff as a whole. Time is set aside each year to review standards, monitor curriculum provision and ensure that training, safeguarding arrangements and resources remain up to date.

Intent

At Read St. John's we follow the National Curriculum for Computing. We believe that a high-quality computing education equips pupils to use computational thinking and creativity to understand and change the world. Computing has strong links with mathematics, science, design and technology and many other areas of learning. The core of computing is computer science, in which pupils are taught the principles of information and computation, how digital systems work, and how to put this knowledge to use through programming.

Building on this knowledge and understanding, pupils are equipped to use information technology to create programs, systems and a range of digital content. Computing also ensures that pupils become digitally literate: able to use technology confidently, critically, creatively, positively, responsibly and safely at a level suitable for their age and for future participation in an increasingly digital world.

We recognise that technology is embedded in children's lives and that effective education is central to preventing and reducing online harm. We aim to give pupils the knowledge, vocabulary, judgement and confidence to make safe choices, seek help when needed and understand that digital actions can have consequences. We also recognise the accessibility and inclusion opportunities technology can provide and encourage staff to use computing and digital tools across the curriculum where they enhance learning.

Implementation

At Read St. John's we use the National Centre for Computing Education (NCCE) Teach Computing Curriculum as the basis for our planning, adapting resources where appropriate to meet the needs of our pupils and our school context. Cross-curricular links are made where they strengthen learning without weakening the subject-specific knowledge and progression of computing.

Children learn computing through planned lessons and through purposeful application of their knowledge and skills across the curriculum. A progressive scheme of learning is set out in the school's separate computing skills progression document and topic map. The Teach Computing taxonomy organises learning across ten strands: Algorithms, Networks, Computing Systems, Creating Media, Data and Information, Design and Development, Effective Use of Tools, Impact of Technology, Programming, and Safety and Security.

EYFS Curriculum

Computing in Reception is developed through play, purposeful use of technology, talk, exploration and adult-led opportunities across the areas of learning. Children begin to recognise technology in the world around them, make simple choices when using digital devices, develop early problem-solving skills and learn age-appropriate messages about privacy, asking for help and staying safe when using technology.

National Curriculum

KS1

The children will be taught to:

- understand what algorithms are; how they are implemented as programs on digital devices; and that programs execute by following precise and unambiguous instructions (1.1)
- create and debug simple programs (1.2)
- use logical reasoning to predict the behaviour of simple programs (1.3)
- use technology purposefully to create, organise, store, manipulate and retrieve digital content (1.4)
- recognise common uses of information technology beyond school (1.5)
- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies (1.6)

KS2

The children will be taught to:

- design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts (2.1)
- use sequence, selection and repetition in programs; work with variables and various forms of input and output (2.2)
- use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs (2.3)
- 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 (2.4)
- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content (2.5)
- select, use and combine a variety of software, including internet services, on a range of digital devices to design and create programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information (2.6)
- use technology safely, respectfully and responsibly; recognise acceptable and unacceptable behaviour; identify a range of ways to report concerns about content and contact (2.7)

Online Safety, Digital Citizenship and Artificial Intelligence

Online safety is taught as a whole-school and cross-curricular responsibility, supported strongly through Computing and Relationships/Health Education. Teach Computing online-safety resources and other authoritative materials are used alongside the computing curriculum where they strengthen age-appropriate teaching.

Pupils are taught to behave respectfully online; protect personal information; understand privacy and location settings; recognise that online content and communication can be copied or shared; critically evaluate online relationships and sources of information; recognise harmful content or contact; and know how, when and where to report concerns and seek help.

Pupils are also introduced, in an age-appropriate way, to artificial intelligence (AI), including examples of where AI is used in everyday life. Teaching helps pupils understand that AI-generated content can be inaccurate, biased, misleading, out of date or inappropriate and therefore needs to be checked critically rather than accepted automatically. Pupils are taught not to enter personal or confidential information into unapproved digital or AI tools.

Where generative AI is used in school, its use must have a clear educational purpose, comply with age restrictions and school procedures, and be considered in relation to safeguarding, filtering and monitoring, data protection, intellectual property and its possible impact on learning. Pupil-facing use will only take place with appropriate safeguards and supervision.

Spiritual, Moral, Social and Cultural Development

Spiritual development: Computing provides opportunities for pupils to reflect on creativity, human ingenuity and the changing possibilities of technology. Pupils are encouraged to consider the role technology plays in their own lives and the wider world, while developing confidence, curiosity, perseverance and a sense of achievement.

Moral development: Pupils consider responsible and irresponsible uses of technology, including privacy, personal data, online behaviour, cyberbullying, copyright, misinformation, AI-generated content and the consequences of digital choices. They are taught that access to technology brings responsibilities as well as opportunities. Relevant teaching is informed by current data protection law, the Computer Misuse Act and copyright legislation.

Social development: Computing gives pupils opportunities to communicate, collaborate, solve problems and create for different audiences. Pupils learn to listen to the ideas of others, work constructively in groups and use digital tools respectfully. They also learn that the standards of behaviour expected face-to-face apply online.

Cultural development: Pupils explore how developments in computing and digital communication influence culture, work, creativity, communities and global connections. They consider how technology can widen access and communication while also recognising that digital content can reflect bias, stereotypes and unequal representation.

Assessment, Monitoring and Moderation

Assessment is an integral part of the teaching process and is used to inform planning and identify next steps. Teachers assess pupils' understanding and application of computing knowledge and skills through observation, questioning, discussion, practical outcomes, digital work and appropriate unit or end-of-year assessment. Judgements are made against the curriculum expectations and the school's progression of skills.

Feedback is given as close to the learning as possible and is guided by the school's feedback and marking approach. Pupils are encouraged to make links between current learning and previous knowledge and to use subject-specific vocabulary accurately.

Monitoring and moderation takes place regularly through:

- monitoring of planning and curriculum coverage
- learning walks and observations
- scrutiny of books and digital work
- moderation of work and assessment
- discussions with pupils and pupil voice questionnaires
- staff meetings, staff audits and professional development
- review of online-safety curriculum coverage and emerging needs
- meetings and/or observations with the nominated governor.

Safeguarding and Online Safety

Online safety is an integral part of safeguarding. This policy should be read alongside the school's Safeguarding and Child Protection Policy, behaviour arrangements, acceptable-use procedures, data-protection policies and any relevant mobile-phone or personal-device arrangements. All staff share responsibility for keeping children safe online and for reporting concerns through the school's safeguarding procedures.

The school follows the current Keeping Children Safe in Education guidance. Online-safety risks are considered through the four broad areas commonly referred to as the 4Cs:

- Content - exposure to illegal, inappropriate or harmful material, including misinformation and disinformation.
- Contact - harmful interaction with other users, or with generative AI applications that simulate interaction.

- Conduct - behaviour online that causes or increases the likelihood of harm, including online bullying and the creation or sharing of harmful or explicit material, including material generated or altered using AI.
- Commerce - risks such as scams, phishing, inappropriate advertising and gambling-related content.

Online safety is treated as a running and interrelated theme across safeguarding, curriculum planning, staff training and communication with parents and carers. Pupils are taught that concerns about something seen, received or experienced online should be reported to a trusted adult, and staff follow the school's safeguarding procedures when concerns arise.

Filtering and Monitoring

The school maintains appropriate filtering and monitoring arrangements for school networks and devices. Netsweeper is used as part of the school's web-filtering provision. Filtering is complemented by appropriate monitoring strategies and active staff supervision so that concerning online activity can be identified and responded to.

In line with current Department for Education expectations, roles and responsibilities for filtering and monitoring are clearly assigned. The effectiveness of the school's filtering and monitoring provision is reviewed at least once every academic year by the responsible member of the senior leadership team, supported by the Designated Safeguarding Lead and IT support. The review includes checks that filtering is working appropriately on internet-connected devices in relevant locations, and a record of the checks and actions is retained.

The annual review considers the age and needs of pupils, including those who may be at greater risk of harm, how school technology is used, the balance between safeguarding and appropriate access for learning, and whether systems can respond effectively to changing risks, including AI-generated or dynamic content.

Artificial Intelligence and Safeguarding

The school recognises that generative AI can create new safeguarding, data-protection and intellectual-property risks. Staff and pupils must only use AI tools in accordance with school expectations. When a new AI tool is considered for use, the school will consider its intended purpose, age suitability, privacy and data handling, filtering and content moderation, monitoring and reporting features, accuracy, bias, security and the impact on pupils' learning and development.

Any content produced using generative AI requires critical checking for accuracy, appropriateness and bias. Personal, sensitive or confidential information about pupils, families or staff must not be entered into unapproved AI systems. Where pupil-facing AI is used, pupils will be supervised appropriately and taught how to question outputs rather than treat them as authoritative.

Staff Training and Responsibilities

All staff receive safeguarding and child-protection training at induction, including online safety and an understanding of the school's filtering and monitoring arrangements. Training is regularly updated and staff receive online-safety and safeguarding updates at least annually, with additional updates when risks, technology or guidance change. Staff know how to escalate concerns to the Designated Safeguarding Lead.

Parents and Carers

The school uses communication with parents and carers to reinforce key online-safety messages, including age-appropriate use of online services, privacy, reporting routes, emerging risks and the school's approach to filtering and monitoring. Where pupils are asked to use online services for learning, parents and carers should be given clear information where appropriate about the purpose of the service and how it is used.

Resources

- Classrooms have access to desktop computers and centrally located laptops, tablets and iPads.
- Bee-Bots and Pro-Bots, LEGO WeDo, LEGO Mindstorms, K'NEX, FlowGO, Makey Makey, micro:bits and microphones are available to support the computing curriculum.

- A range of software and online services is used to support curriculum delivery, including resources such as Scratch, Tinkercad, coding tools and STEM resources. Services are reviewed for suitability before use.
- Equipment is maintained and repaired with support from the school's IT technician/provider.
- Netsweeper is used as part of the school's web-filtering provision, alongside appropriate monitoring and safeguarding procedures.
- Jam Coding provides an extra-curricular weekly club for learners.
- The subject leader makes regular use of current NCCE/Teach Computing resources and CPD, including support for primary computing, online safety and AI, alongside appropriate DfE, UKCIS, UK Safer Internet Centre, ProjectEVOLVE and other authoritative guidance.
- Staff are provided with computing and online-safety training through staff meetings, INSET and relevant CPD according to identified need. The subject leader has achieved the National Centre for Computing Education Certificate in Primary Computing Teaching.

Impact

Pupils are digitally literate and can discuss, reflect on and appreciate the impact that computing and technology have on learning, development, wellbeing and wider life. They make increasingly informed choices about technology, understand how to use it safely and responsibly, and can explain appropriate actions when something online causes concern.

Pupils use computing vocabulary with growing accuracy and show confidence, perseverance, resilience and creativity. They achieve the objectives appropriate for their year group, or their individual plan where this differs, and take pride in the work they create, present, share and evaluate.

By the end of KS2, pupils should:

- understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation
- analyse problems in computational terms and have repeated practical experience of writing computer programs in order to solve such problems
- evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems
- be responsible, competent, confident, critical and creative users of information and communication technology
- recognise common online risks, make sensible decisions about privacy and communication, critically evaluate digital information and know how to report concerns and seek help
- have an age-appropriate understanding of artificial intelligence and recognise that AI-generated content needs to be checked for accuracy, bias, safety and reliability.

Key Guidance and Resources

- National Curriculum in England: Computing programmes of study
- Teach Computing Curriculum - National Centre for Computing Education
- Teach Computing - Primary online safety resources
- Teach Computing - AI in primary computing
- Keeping Children Safe in Education 2026
- DfE Filtering and Monitoring: core standard
- Relationships Education, Relationships and Sex Education (RSE) and Health Education - statutory guidance
- DfE Generative artificial intelligence in education
- DfE Generative AI: product safety standards

This policy was updated in September 2026 and will be reviewed in September 2027, or sooner if there are significant changes to statutory guidance, the school's technology provision or identified safeguarding risks.