St. Edward's Computing and E-safety policy

Last review date: 2 July 2020

Approved by Senior Management Team: 2 July 2020

Ratified by Governing Body: 14 July 2020

Next review date: September 2021

Computing

Introduction

This policy sets out St. Edward's aims and strategies for the successful delivery of Computing using Purple Mash and working alongside Warwickshire ICTDS. The policy has been developed by the Computing Leader (Mr Phillips) in consultation with the SENCO, Leadership Team and teachers. Guidance from consultants and pupil and staff voice questionnaires will continue to help shape this policy. This policy is based on government recommended/statutory programme of study. Our Policy has been written by the school, building on the Warwickshire ICT Development Service e-safety Policy and Purple Mash scheme. It has been agreed by the senior management and approved by governors. Due to the fast pace of technology innovation and constantly emerging trends, it is recommended that this policy is reviewed, at minimum, at the start of every academic cycle.

Aims

St. Edward's School believes that every child should have the right to a curriculum that champions excellence; supporting pupils in achieving to the very best of their abilities. We understand the immense value technology plays not only in supporting the Computing and whole school curriculum but overall in the day-to-day life of our school. We believe that technology can provide: enhanced collaborative learning opportunities; better engagement of pupils; easier access to rich content; support conceptual understanding of new concepts and can support the needs of all our pupils.

St Edward's aims are:

- Provide an exciting, rich, relevant and challenging Computing curriculum for all pupils.
- Teach pupils to become responsible, respectful and competent users of data, information and communication technology.
- Provide technology solutions for forging better home and school links through use of Homeroom, school twitter account and WeLearn/PurpleMash accounts.
- Enthuse and equip children with the capability to use technology throughout their lives.
- Utilize computational thinking beyond the Computing curriculum.
- Give children access to a variety of high-quality hardware, software and unplugged resources these include desktop computers and I-pads.
- Equip pupils with skills, strategies and knowledge that will enable them to reap the benefits of the online world, whilst being able to minimize risk to themselves or others.

Curriculum

As a school, we have chosen the Purple Mash Computing Scheme of Work from Reception to Year 6. The scheme of work supports our teachers in delivering fun and engaging lessons which help to raise standards and allow all pupils to achieve to their full potential. We are confident that the scheme of work more than adequately meets the national vision for Computing. It provides immense flexibility, strong cross-curricular links. Furthermore, it gives excellent supporting material for less confident teachers. At St. Edward's, our intention is for each year group to be taught online safety and coding each academic year. This will be alongside other aspects that cover a balanced range of the computing curriculum.

Early Years

Early Years We aim to provide our pupils with a broad, play-based experience of Computing in a range of contexts. We believe the following:

- Recording devices can support children to develop their communication skills. This is especially useful for children who have English as an additional language.
- Early Years learning environments should feature ICT scenarios based on experience in the real world, such as in roleplay.
- Pupils gain confidence, control and language skills through opportunities to 'paint' on the interactive board/devices or control remotely operated toys.
- Outdoor exploration is an important aspect, supported by ICT equipment.

Key Stage 1

- Understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following a sequence of instructions.
- Write and test simple programs.
- Organize, store, manipulate and retrieve data in a range of digital formats.

- Communicate safely and respectfully online, keeping personal information private, and recognize common uses of information technology beyond school.

Key Stage 2

- Design and write programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts.
- 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.
- 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.
- Select, use and combine a variety of software (including internet services) on a range of digital devices to accomplish given goals, including collecting, analyzing, evaluating and presenting data and information.
- 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 worldwide web; and the opportunities they offer for communication and collaboration.

Assessment

- Pupil attainment is assessed using O Track for Years 1 to 6. The tool enables staff to accurately identify attainment of pupils through the detailed exemplification it has for each key learning intention.
- Work from a range of abilities is shared within year group journals to showcase examples of progress, achievement and coverage.
- Formative assessment is undertaken each session/interaction in Computing and pupils are very much encouraged to be involved in that process. Through using the progression of skills documents and displays from 2Simple, both teachers and pupils can evaluate progress. Features such as preview and correct in Purple Mash are used to further support feedback and assessment.
- Children are encouraged to self, peer and group assess work in a positive way using online collaborative tools in Purple Mash.

Monitoring, feedback and evaluation

Monitoring standards of teaching and learning within Computing is the primary responsibility of the Computing Leader. All teachers are expected to include work in year group portfolio for the subject. Details of monitoring and evaluation schedules can be found in the Computing Action Plan and School Monitoring Schedule.

St Edward's will monitor through:

- Work scrutiny/learning walks.
- Pupil/teacher voice.
- Learning environment monitoring.
- Dedicated Computing leader time.

Evaluation and Feedback will be achieved through:

- Using recognized national standards for benchmarking Computing provision.
- Written feedback on evaluation of monitoring activities to be provided by the Computing Leader in a timely manner.
- Feedback on whole school areas of development in regard to Computing to be fed back through insets/staff meetings.

E-Safety

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for Computing and for child protection. The school has appointed a Computing subject lead (Mr Phillips). They will liaise with the Designated Child Protection Coordinator (Head teacher) as the roles overlap. Our E-Safety Policy has been written by the school, building on the Warwickshire ICT Development Service e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors. The e-Safety Policy will be reviewed annually.

Online safety has a high profile at St Edward's for all stakeholders. We ensure this profile is maintained and that pupil needs are met by the following:

- A relevant up-to-date Computing curriculum which is progressive from Early Years to the end of Year 6. A curriculum that requires each year group to have online safety as a unit.
- Through our home/school links and communication channels, parents are kept up to date with relevant online safety matters, policies and agreements. E-safety tips to be shared with parents on school newsletter.
- Data policies which stipulate how we keep confidential information secure.
- Pupils, staff and parents have Acceptable Use Policies which are signed and copies freely available.
- Training for staff and governors which is relevant to their needs and ultimately positively impacts on the pupils.
- Our online safety policy clearly states how monitoring of online safety is undertaken and any incidents/infringements to it are dealt with.
- Scheduled pupil voice sessions and learning walks steer changes and inform training needs.
- Any e-Safety training programme will be taught within lessons across age groups as part of the curriculum and awareness days.

Pupils will be taught how to evaluate Internet content

If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Warwickshire ICT Development Service, and, where appropriate, the school e-safety officer. Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read.

MANAGING INTERNET ACCESS

- Information system security. The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses the Warwickshire Broadband with its firewall and filters.
- The school provides an additional level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Services.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Use of words included in the Policy Central 'banned' list will be detected and logged.
- E-mail sent to an external organization will be written carefully and authorized before sending, in the same way as a letter written on school headed paper.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site or social media.
- Pupil's work is chosen carefully before publishing e.g. If containing personal information.

Social networking and personal publishing.

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc. □

- On school entry a parents' pack will be issued containing safety advice, our school ICT rules and age-appropriate pupil and parent agreement forms.
- The school has a 'Twitter' and 'Homeroom' page that can interact and communicate with parents. This account is set to 'private'. Only people who have been accepted by school administrators to the page can view the material.
- Written permission from parents or carers will be obtained before photographs of pupils are published.

Managing filtering

- The school will work in partnership with the Warwickshire ICT Development Service and BECTA to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils should not bring or use mobile phones at school or on school trips, unless previously arranged with the head teacher. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Authorizing Internet access: All staff and pupils are granted Internet access, although access could be denied in the event of inappropriate use.
- At Key Stage 1 and 2, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- Neither the school nor WCC can accept liability for the material accessed, or any consequences of Internet access.
- The head teacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Sanctions within the school include: – interview/counselling by class teacher or head teacher; – informing parents or carers; – removal of Internet or computer access for a period.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.