Raysfield Primary

Know myself. Respond to my world.
Connect with my community.

Raysfield Primary School

ACCEPTABLE USE POLICY 2021

Signed (Chair):	Name: David Champion	Date: 27.01.2021
Signed (Head):	Name: Claire Hill	Date: 27.01.2021
Ratified: by Standards Committee		Next Review: 3 years – January 2024

Equality Impact Assessment (EIA) Part 1: EIA Screening

Policies, Procedures or Practices	Acceptable Use Policy	Date	27.01.2021
EIA CARRIED OUT BY:	Claire Hill	EIA APPROVED BY:	Standards

Groups that may be affected:

Are there concerns that the policy could have a different impact on any of the following groups? (Please tick the relevant boxes)	Existing or potential adverse impact	Existing or potential for a positive impact
Age (young people, the elderly; issues surrounding protection and welfare, recruitment, training, pay, promotion)		✓
Disability (physical and mental disability, learning difficulties; issues surrounding access to buildings, curriculum and communication).		✓
Gender Reassignment (transsexual)		✓
Marriage and civil partnership		✓
Pregnancy and maternity		✓
Racial Groups (consider: language, culture, ethnicity including gypsy/traveller groups and asylum seekers)		✓
Religion or belief (practices of worship, religious or cultural observance, including non-belief)		✓
Gender (male, female)		✓
Sexual orientation (gay, lesbian, bisexual; actual or perceived)		✓

Any adverse impacts are explored in a Full Impact assessment

School Acceptable Use Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers & visitors) who have access to and are users of school IT systems, both in and out of school.

Technologies open up new learning opportunities and can promote creativity, effective learning and communication. They can promote more effective communications between parents / carers and the school in order to support young people with their learning.

Core Principles:

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. This contributes to development of the key area of developing pupils' skills linked towards future economic well-being.
- Internet use is a part of the statutory curriculum and is a necessary tool for staff and pupils.
- Everyone in the school community has a personal responsibility to work towards keeping themselves and others safe online.
- All users are responsible for making sure they use technology safely, responsibly and legally.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

Infrastructure

- School IT systems capacity and security will be reviewed regularly. Internet access is provided through the South West Grid for Learning which is a filtered service. It is designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- The school cannot be held responsible for the nature and content of materials accessed using technology as security systems cannot protect against everything.
- Virus protection is provided by the South Gloucestershire Education IT team and our contract states that it is updated regularly.
- Security strategies will be periodically discussed with the LA and an annual audit (see appendix 1) will be carried out.

Policy and Practices Roles and Responsibilities

- The school has appointed an e-safety co-ordinator who will manage and monitor e-safety.
- The IT technician regularly monitors internet access and brings any issues to the attention of the e-safety co-ordinator who then takes appropriate action.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. The school will work with the LA, SWGfL, DfCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- The school has clearly set out roles and responsibilities in relation to internet use and these can be seen in Appendix 1.

Auditing Issues

- Pupil surveys regarding e-Safety are completed as required and issues are identified and followed up in teaching.

Issues, Misuse and Complaints

- Any e-safety issues are logged and dated and the action taken is also recorded on CPOMS. This includes information about the nature of the incident, who was involved and how it was dealt with. This log is reviewed to identify any trends in issues that may need addressing.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator, who will immediately report it to SWG to ensure it is filtered out.
- Complaints of internet misuse will be dealt with by a senior member of staff and any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- All staff will have their own individual logins and password. Staff must not share passwords as individual logins can be used to monitor any action taken when logged on. Every user is individually responsible at all times for the action taken while their user name is in use. Users need to be aware that if their password is shared someone else could use it to take action that could be tracked to them.

Education and Training Teaching

Pupils will be taught:

- how to access a given internet site and how to use site navigation
- what internet use is acceptable and what is not and given clear objectives for internet use
- about the different ways that the internet can be used e.g. contacting people, finding information, purchasing etc.
- about the effective use of the internet in research, including the skills of knowledge location, retrieval and begin to evaluate sources
- how to carry out internet searches in order to reduce the risk of accessing inappropriate material
- about the effective and acceptable use of internet for web publishing where appropriate.
- about the safe use of the internet to support communications
- about what to do if they encounter a problem.

Teaching about the issues is mapped in to our IT curriculum to ensure that pupils have relevant learning experiences and a scheme of work identifies what is taught during each year.

Managing Internet Access for Teaching

- Staff and pupils will receive training on how to carry out internet searches safely and efficiently.
- Pupils will not carry out internet searches unless they have first been tested by a teacher/ adult to ensure that they do not produce results containing inappropriate material.
- Access to the internet will be directly supervised with access to specific, approved on-line materials.
- 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. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Parents will be asked to sign and return the school's Internet Acceptable Use Partnership Agreement.

Training

- The e-safety co-ordinator will attend regular training in order to keep up to date with the latest recommendations.
- There will be regular briefings for staff. Staff will receive training on how to carry out internet searches safely and efficiently and minimise risk.
- There will be the opportunity for parents to attend e-safety workshops.

All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

Technology Specific Issues

Electronic Communications, for example, e-mail and text

- Pupils may only use approved class e-mail accounts on the school system.
- Staff must read and check the content of all class e-mails before using with pupils. E-mails must be treated as 'public'.
- Pupils must not reveal personal details of themselves or others in any online communication, or arrange to meet anyone.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- All must be polite and considerate online and report any issues that are likely to cause offence to others.

Social networking and personal publishing

- The school will block/filter access to open social networking sites and give access only to those sites that are monitored and approved by South West Grid recommendations, this includes online platforms.
- Tools including message boards, blogs, instant messaging and collaboration tools will be used in this safer, closed environment. Children will be taught how to safely communicate and publish content in a closely supervised and supported way.
- All communication will be treated as 'public'.
- Newsgroups will be blocked unless a specific use is approved.
- Staff are advised not to make contact with parents or children through social networking sites or via personal e-mail addresses but only through agreed school systems. Staff are advised to refuse any friend requests that are made.

Published content and the school web site

- The contact details on the school website and social media pages should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Children and members of staff may use digital cameras to record learning activities. These images may be used in lessons or to celebrate success through being published in newsletters, on the school website or occasionally in the public media.

- The school will comply with the Data Protection Act and ask parental permission before taking and using images. The school will also ensure that when images are published the young people cannot be identified by the use of their full names.
- Parents can contact the school if they decide to withhold permission.
- Photographs that include pupils will be selected carefully.

Use of iPads in school

- Only apps with educational benefit will be allowed to be installed.
- Apps are only installed by South Gloucestershire IT under the direction of the IT Leader.
- Internet access is only available via a login.

Managing video-conferencing

- Video-conferencing must only be used via the schools recommended platform.
- Refer to video-conferencing policy.

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.

Behaviour

- Children are expected to behave well online as they are expected to during all other school activities.
- Bullying is not tolerated in any form and this includes online.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Conclusion

Access to the internet and digital communication media have the potential to greatly enhance learning and engagement with parents and our school is committed to extending these opportunities whilst maintaining the highest standards of safety. Everyone in school has a personal responsibility to work towards keeping themselves and others safe online.

We take opportunities to maximize positive impacts for sexuality, disabled and non-disabled people, people of different ethnic, cultural and religious backgrounds, girls, boys, men and women.

Appendix 1: E-Safety Audit

This quick self-audit is used to help the senior management team (SMT) assess whether the e-safety basics are in place and enables us to monitor safety.

Has the school an e-Safety Policy that complies with CFE guidance?	Y
Date of latest update: 27th January 2021	
The Policy was agreed by governors on: 27th January 2021	
The Policy is available for staff at: www.raysfield.org.uk	
And for parents at: www.raysfield.org.uk	
The Designated Child Protection Coordinators are: Claire Hill & Sarah Thomas	
The e-Safety Coordinator is: Sarah Thomas	
Have roles and responsibilities in relation to e-safety been clearly identified?	Y
Has e-safety training been provided for both students, staff and parents? How frequently? Has it highlighted any issues?	Y
Do all staff sign an Acceptable use agreement?	Y
Do parents sign and return an agreement that they support the School e-Safety Rules?	Y
Have school e-Safety Rules been set for pupils which have been discussed with them?	Y
Are these Rules displayed in all rooms with computers?	Y
Internet access is provided by an approved educational Internet service provider and complies with DCfS requirements for safe and secure access (e.g. SWGfL).	Y
Has an ICT security audit has been initiated by SMT, possibly using external expertise?	N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y
Has monitoring of internet use taken place with any issues being logged?	Y
Has an e-safety log been completed and reviewed to identify and issues which need to be addressed?	Y
Relevant pupil surveys have been completed and issues have been identified and addressed through teaching	Y