ROWAN GATE PRIMARY SCHOOL

APPROPRIATE USE OF THE INTERNET AND TECHNOLOGY POLICY

POLICY REVIEW

This policy has been reviewed in line with the following: (Reviewer please tick box)

a) Ensuring the policy is up to date and meets mandatory requirements [√]

b) Ensuring the policy is fit for purpose and that practice adheres to the policy. [√]

Reviewed and Updated in March 2022 ……..

Print Name Natalija Zemcugova

Policy will be reviewed again in **February 2023*.***

ROWAN GATE PRIMARY SCHOOL

APPROPRIATE USE OF THE INTERNET AND TECHNOLOGY

This school policy reflects the consensus of opinion of the whole teaching and support staff and has the full agreement of the governing body.

"This policy reflects the philosophy of the Equality Policy, the Mission Statement and the School Aims in relation to the whole curriculum".

We all share the responsibility to make sure that children's and adults' use of the Internet is appropriate and safe.

This Policy should be read in conjunction with the school's Computing Policy and must be used in line with General Data Protection Regulations - GDPR.

1. Introduction

Rowan Gate Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

2. Benefits

- Access to resources from across the world, including art galleries and museums.
- Access to up-to-date information and resources.
- Access to DfE papers, data and initiatives on-line.
- Widening of cultural horizons and exchange of information with peers overseas.
- Access to experts in fields of study.
- Staff professional development, on-line support and challenge.
- Improved data transfer between schools and within the LA.
- Improved access to support and advisory staff, professional associations and colleagues.
- Access for staff to online systems, such as e-mails, CPOMS or Personal Incident report
- Exchange of curriculum and administration data with the LA, DfE and other organisations.

3. Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.
The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. Teachers, parents and pupils need to develop good practice in using the Internet as tool for teaching and learning. There is a fine balance between encouraging autonomous learning and maintaining adequate supervision.

The importance of online safety is integrated across all school operations in the following ways:

- Staff receive training in the use of the Internet to support their professional development, their lesson preparation and the creation of challenging learning tasks.
- Staff receive email updates regarding any changes to online safety guidance or legislation
- Staff pre-select sites which support the learning outcomes planned for the pupils' age, maturity and ability.
- Online safety is integrated into learning throughout the curriculum.

4. Handling Online Safety Concerns

The school's network and school-owned devices are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the headteacher who manages the situation in line with the Child Protection and Safeguarding Policy.

When using Internet, the following rules need are applied:

- Pupils are supervised at all times. This may include supervision by teachers or support staff. Students on placements should not supervise pupils using the Internet or sending emails.
- When pupils are accessing the internet, it is necessary that the screen in fully visible.

In addition to this, teachers will

- Quickly address any specific issues related to online safety that arise within their year groups;
- Address online safety in circle times and PSHE lessons

The technical strategies being developed to restrict access to inappropriate material fall into two overlapping types (sometimes all referred to as filtering): Blocking strategies remove access to a list of unsuitable sites or newsgroups. The school can also add inappropriate sites to this list. Filtering examines the content of web pages or e-mail messages for unsuitable words. Blocking and/or filtering, as previously stated, is performed by Quantum Surfprotect monitoring software. This software identifies all internet use and flags up any inappropriate searches and/or risky sites to ensure that pupils use of the internet is appropriate and safe.

If staff discover unsuitable material, the URL and the content must be reported without delay to the Internet Service Provider by the head teacher. Any material that the school suspects is illegal will also be referred to the SLT.

The school will work closely with parents; the Local Authority, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and continuously improved.
Deviation from the school rules could include minor misdemeanours as well as the potentially serious and a range of sanctions will be required, linked to the schools' behaviour policy.

A member of the SLT will ensure that all staff and pupils are aware of the correct pathway for handling individual pupils' or parents' complaints.

Any warnings flagged by Quantum Surfprotect monitoring software will be investigated, followed-up and recorded in line with safeguarding procedures.

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to SLT, who investigate concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manage concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Child Protection and Safeguarding Policy. Parents will always be informed when inappropriate ICT use occurs.
Sanctions available will include counselling by pastoral member of staff attached to individual pupil, in association with pastoral member of the SLT.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.
The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.
All online safety incidents and the school's response are recorded on CPOMS.

5. Why we need an appropriate use policy

The Government wants everyone to have access to the wealth of cultural, scientific and intellectual material available online, so the existence of undesirable material is not a valid reason to avoid the Internet. Therefore, it is necessary for all members of staff to be aware of the issues surrounding the use of the Internet for education.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. In line with Northamptonshire local authority policy Rowan Gate Primary School will provide a filtered Internet service through EMBC.

However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a school machine. No system can be completely effective and a combination of approaches will be required in addition to adequate supervision. All staff, governors, parents and advisers will work to establish agreement that every reasonable measure has been taken.

Due to the process involved in publishing information on the Internet, it is not possible to guarantee that unsuitable material will never appear on a computer screen.

Neither the school nor the Northamptonshire local authority is able to accept liability for the materials accessed, or any consequences thereof.

The school will work in partnership with parents, the Local authority, DfE and the Internet Service Provider (ISP) to ensure systems to protect pupils are reviewed and improved.

Members of the School's Senior Leadership team will ensure periodic checks are made to substantiate that the filtering methods employed are effective in practice.

If unsuitable sites are discovered by anyone belonging to the school community, a member of staff will report the URL to the head teacher who will report the address and content without delay to the Internet Service Provider.

6. Online Safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy and the Child Protection and Safeguarding Policy.

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The Computing Coordinator and PSED Coordinator will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

6. Use of Internet/ Online Safety and the Curriculum

Internet access is a necessary part of the statutory curriculum. It is an entitlement for pupils based on their responsible use.

Access to the Internet is required to fulfil the requirements of the national curriculum. All pupils will be provided with the minimum access required

At KS1, the majority of access to the Internet will be by a teacher or by adult demonstration. At other times pupils will have supervised access to specific pre-selected and approved sites.

At KS2, Internet access will be required as part of the Curriculum Programme of Study, following education in responsible and appropriate use.

Staff will have open, but monitored Internet access for research purposes and continued professional development. All staff will be advised of the conditions of their use of the Internet. Inappropriate use will be considered a disciplinary issue.

Parents of all pupils will be asked to sign and return a permission form, without this permission form a pupil is unable to access the Internet. The school will keep a record of pupils' acceptance of the policy

Online safety is integrated into learning throughout the curriculum. Pupils are educated in taking responsibility for Internet access and appropriate use in a differentiated way. As part of the curriculum children learn to 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. This statement covers the key principles of pupils' e-safety. Pupils should be aware of the main risks associated with the internet, and recognise that they should not share certain types of personal information online. They are allowed to search the Internet under supervision for information and resources to meet their learning objective.

Online safety teaching is always appropriate to pupils' ages and developmental stages.
Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

6. Use of Technology in the Classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets/ Ipads
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.
Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.
Pupils will not be permitted to use smart devices or any other personal technology whilst on school site.

Staff will use all smart technology and personal technology in line with this Policy.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.
The school will consider the 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

7. How emails are managed

Email is an essential means of communication within education. Access to and the use of emails is managed in line with the Data Protection Policy and Use of Internet and Technology Policy.
The capacity to use email is an important means of communication in society; pupils should learn to effectively use it as they do other forms of written communication. Email can inspire otherwise reluctant writers to concentrate on their spelling and grammar in order to send messages to peers. It can help pupils make the transition between schools or enable direct access for pupils away from school. Email extends communication beyond the school, into the home, the workplace and the community.

Once email is available it is difficult to control its content. Nevertheless, email content should not be considered private.

Pupils are required to use email as part of the National Curriculum.

Email in school must only be used for educational purposes.

Messages sent from a school computer should be regarded in the same way as messages written on headed paper.

Staff and pupils are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Personal email accounts are not permitted to be used on the school site.

Any email that contains sensitive or personal information is only sent using secure and encrypted email (Egress).
The school uses Microsoft Office 365 platform for staff and pupils.
All pupils have access to their Class Team, where they can use Posts, Files and Assignments.
The use of chat rooms is not allowed from that platform for pupils. However, the use of professional discussion groups is permitted for staff.

The sending of offensive messages or pictures is not allowed.

Staff members and pupils are required to block spam and junk mail, and report the matter to ICT technicians (easipc). The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

Any cyber-attacks initiated through emails are managed in line with the Data and Cyber-security Breach Prevention and Management Plan.

8. Individual Responsibilities

All school-based employees, including volunteers under the age of 18, must:

- take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly.

- ensure that children and young people in their care are protected and supported in their use of technologies so that they can be used in a safe and responsible manner. Children should be informed about what to do in the event of an e-Safety incident.

- report any e-Safety incident, concern or misuse of technology to the member of SLT, including the unacceptable behaviour of other members of the school community.

- Only use school issued email addresses, mobile phones and cameras to take, save or send sensitive pupil data or images/video footages of students by employees unless specific written permission to use a personal device has been granted by the Head Teacher, for example, due to equipment shortages.

- ensure that all electronic communication with pupils, parents, carers, employees and others is compatible with their professional role and in line with school protocols. Personal details, such as mobile number, social network details and personal e-mail should not be shared or used to communicate with pupils and their families.

- Not use personal details, such as mobile number, social network details and personal e-mail should not be shared or used to communicate with pupils and their families.

- Not use personal technology (This includes, but is not limited to smart phones, Ipads, smart watches etc.) for personal use, in directed hours or in front of pupils.

- Not post online any text, image, sound or video which could upset or offend any member of the whole school community or be incompatible with their professional role.

- Understand that behaviour in their personal lives may impact upon their work with those children and young people if shared online or via social networking sites (this includes, but is not limited to written content, videos or photographs, and views expressed either directly or by 'liking' certain pages or posts established by others etc).

- Not list Rowan Gate Primary School as their place of employment on any social media

- Obtain permission from SLT before posting anything that has reference to the school on social media – this should only be Rowan Gate account on FB.

- protect their passwords/personal logins and log-off the network wherever possible when leaving work stations unattended.

- understand that network activity and online communications on school equipment (both within and outside of the school environment) may be monitored, including any personal use of the school network. Specific details of any monitoring activity in place, including its extent and the manner in which it is carried out, should be detailed in the school's local IT Policy.

- understand that employees, who ignore security advice or use email or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.

However, please note that:

- Use of obscene language, which harasses, insults or abuses others is not permitted.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Closed discussion groups can be useful but the use of public chat rooms is not allowed.
- Personal emails such as Yahoo or Hotmail should not be accessed whilst connected to the school network.
- Employees, who ignore security advice or use technology or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.
- Members of staff are reminded that they should not deliberately seek out inappropriate /offensive materials on the Internet and that they are subject to the Local Authority's recommended disciplinary procedures should they do so.

9. The management of the School Website

The school website can celebrate pupils' work, promote the school and publish resources for projects or homework. Ground rules are important to ensure that the Web site reflects the school's ethos and that information is accurate and well presented. As the school's Web site can be accessed by anyone on the Internet, the security of staff and pupils must be considered carefully. While any risks might be small, the parents' perception of risk has been considered in the devising of this policy.

- The Head Teacher/SLT will delegate editorial responsibility to members of staff to ensure that content is accurate and quality of presentation is maintained. The school website will be the responsibility of the PA to the headteacher. Other staff are responsible for supplying suitable items for the PA to upload.
- All material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name.
- The point of contact on the web site should be the school address and telephone number. Home information or individual e-mail identities will not be published.
- Written permission from parents will be sought before photographs or pupils work are published on the school web site.

10. The maintenance of security of the ICT systems

The Internet is a connection to the outside world that could compromise system performance or threaten security.
Security strategies will be put in place in line with LA and GDPR procedures.
Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians. Firewalls are switched on at all times. ICT technicians review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to ICT technicians.

Personal data should not be sent over the Internet from school except in secure files, e.g. using Egress secure email.
All members of staff have their own unique usernames and private passwords to access the school's systems. All pupils are provided with their own unique username and private passwords. Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.
Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher is informed and decides the necessary action to take.
Use of e-mail to send and receive attachments will be monitored by Quantum Surfprotect monitoring software.
Users are required to lock access to devices and systems when they are not in use.
Staff should not use school computers to access personal e-mail accounts, i.e. Hotmail, Yahoo mail.

13. Using and Applying the Appropriate Use of the Internet Policy

To ensure all staff working in the school (including supply staff and other visitors) are aware of the schools' Use of Internet and Technology Policy – Rules for responsible Internet use will be printed and posted near all Internet-ready computers in the school.

All staff will be supplied with a copy of the Use of Internet and Technology policy and its importance explained. New members of staff will be briefed at induction meetings.

A module on responsible 'Internet Use' is included in the Computing programme covering both home and school use of the Internet.

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents are sent a copy of the Use of Internet Policy at the beginning of each academic year.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Useful links:

NASUWT Social Networking- Guidelines for Members
http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking

NUT E-Safety: Protecting School Staff- Guidance for Members
http://www.teachers.org.uk/node/12516

UNISON- Guidance on Social Networking
http://www.unison.org.uk/education/schools/pages_view.asp?did=9786

Internet safety sites

Childnet International www.childnet.com

Kidsmart www.kidsmart.org.uk

Digizen www.digizen.org

Thinkuknow www.thinkuknow.co.uk

Netsmartz www.netsmartz.org

WiseKids www.wisekids.org.uk

Wired Kids www.wiredkids.org

Disney www.disney.co.uk/DisneyOnline/Safesurfing

Internet Safety Zone www.internetsafetyzone.com

Review

This policy was reviewed in March 2022 and will be reviewed again in February 2023. This policy was led by Mrs N.Zemcugova