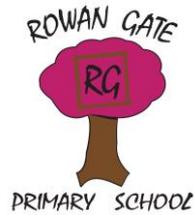


# ROWAN GATE PRIMARY SCHOOL



## A CURRICULUM POLICY FOR THE APPROPRIATE USE OF THE INTERNET

### 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

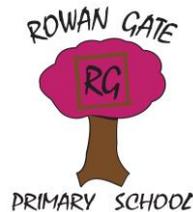
b) Ensuring the policy is fit for purpose and that practice adheres to the policy.

Reviewed and Updated in February 2021 .....

Print Name

Natalija Zemcugova

***Policy will be reviewed again in February 2022.***



## **A CURRICULUM POLICY FOR THE APPROPRIATE USE OF THE INTERNET**

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**

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

Access to the Internet is a necessary tool for the whole school community. It is therefore a requirement as part of safeguarding and GDPR for children and staff to always take responsible and mature approach.

### **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. How will Internet Use support Effective Learning?**

Northamptonshire local authority recommends to Northamptonshire Schools that it is essential to purchase Internet access from a supplier that provides a service designed for pupils. This will include

filtering system appropriate to the age of the pupils. Rowan Gate has conformed to these recommendations and has purchased its broadband access from EXA.

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.

Internet access is an integral part of the use of ICT to support learning and the management of learning.

All staff will be trained in the use of the Internet to support their professional development, their lesson preparation and the creation of challenging learning tasks.

Staff will pre-select sites which will support the learning outcomes planned for the pupils' age, maturity and ability.

Sites that are repeatedly used may be stored in favourites (and added to the URL address book).

Access levels will be reviewed to reflect the curriculum requirement.

Pupils will be educated in taking responsibility for Internet access and appropriate use. As part of the new curriculum children will 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 will be allowed to search the Internet under supervision for information and resources to meet their learning objective.

#### **4. Why do we need an appropriate use policy?**

Pupils in our school are unlikely to see inappropriate content in books due to selection by publishers and teachers. This is not the case with the Internet. The Internet is vast and unregulated, and there remain concerns that it can be abused. Anyone anywhere can publish material on the Internet and it is not censored for opinion bias or validity of information. Children and staff may:

- be exposed to unacceptable materials (pornographic, violent, extremist literature)
- encounter inappropriate messages
- arrange contacts and meetings (potential exploitation and physical dangers)
- inadvertently provide personal information whilst on-line which could be sufficient to put them in danger or to allow commercial companies to exploit them.

The Government wants everyone to have access to the wealth of cultural, scientific and intellectual material available on the Internet, 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. This policy details the way the Internet can and cannot be used.

#### **5. Entitlement - How and why access to the Internet is authorised?**

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

## **6. How will the school ensure the safe use of the Internet in teaching and learning?**

All use of the school's Internet access will be monitored, including that by staff, pupils, governors and parents.

When using the Internet the following rules need to be applied:

- Pupils will be 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 is fully visible.

Teaching of internet safety is a compulsory part of the computing curriculum. As a school, we have our own Internet Safety scheme of work which is part of Computing Curriculum. This scheme of work introduces different concepts related to internet safety in a differentiated way for the pupils and makes good use of a range of recommended online materials.

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.

## **7. How will email be managed?**

Email is an essential means of communication within education. 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.

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.

## **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.
- use school ICT systems and resources for all school related business and communications, particularly those involving sensitive pupil data or images of students. School issued email addresses, mobile phones and cameras must always be used 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.
- Do 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. Individuals working with children and young people must 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.
- 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.
- The use of obscene language, which harasses, insults or abuse to others is not permitted.

## **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 taken into account 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 assessment of risk when using the Internet in school**

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.

## **11. 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.  
The security of the whole system will be reviewed on an ongoing basis.

Personal data should not be sent over the Internet from school except in secure files, e.g. using Egress secure email.

Virus protection and monitoring software will be installed and updated regularly on all machines.

Use of e-mail to send and receive attachments will be monitored by Quantum Surfprotect monitoring software.

Staff should not use school computers to access personal e-mail accounts, i.e. Hotmail, Yahoo mail.

## **12. How will the school handle complaints?**

A complaints procedure will be made available to all staff, parents and pupils and governors. In line with normal school working re discipline matters pupils, parents and staff will need to work together to resolve issues.

Prompt action is taken if a complaint is made or inappropriate use flagged.

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.

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.

Violations of the school rules may lead to a temporary removal of the entitlement to use the e-mail, Internet or/and school computers.

When applicable, police and/or local authorities may be involved. Early contact will be made to establish legal position and discuss necessary strategies.

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

## **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' Acceptable Use 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 Appropriate Use 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.

Parents' attention will be drawn to the policy by letters explaining it.

**Useful links:**

**NASUWT** Social Networking- Guidelines for Members

<http://www.nasuw.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](http://www.unison.org.uk/education/schools/pages_view.asp?did=9786)

**Internet safety sites**

Childnet International [www.childnet.com](http://www.childnet.com)

Kidsmart [www.kidsmart.org.uk](http://www.kidsmart.org.uk)

Digizen [www.digizen.org](http://www.digizen.org)

Thinkuknow [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

Netsmartz [www.netsmartz.org](http://www.netsmartz.org)

WiseKids [www.wisekids.org.uk](http://www.wisekids.org.uk)

Wired Kids [www.wiredkids.org](http://www.wiredkids.org)

Disney [www.disney.co.uk/DisneyOnline/Safesurfing](http://www.disney.co.uk/DisneyOnline/Safesurfing)

Internet Safety Zone [www.internetsafetyzone.com](http://www.internetsafetyzone.com)

**Review**

*This policy was reviewed in February 2021 and will be reviewed again in February 2022. This policy was led by Mrs N.Zemcugova*