ROTHWELL VICTORIA PRIMARY LEARNING PARTNERSHIP

Montsaye Community Learning Partnership

Online Safety & Computing Acceptable Use Policy

Draft Document

September 2018

Rothwell Victoria Infant School

CARE SHARE

HELP SMILE

ROTHWELL JUNIOR SCHOOL

Achievement through Respect Creativity Enjoyment Endeavour

Montsaye Community Learning Partnership

The designated member responsible for internet safety in the school is the Executive Headteacher

The aims of this Policy are to:

- Ensure that pupils benefit from all learning opportunities offered by the internet resources provided by the school in a safe and controlled manner.
- Ensure that all staff and students are aware of online risks and equipped with the necessary skills and knowledge to become responsible digital citizens.
- Ensure that all staff benefit from internet access, with clear guidance on safe and acceptable use, both within the school setting and beyond.
- Make staff and pupils aware that Internet Use in school is a resource and a privilege.
- Provide guidance to staff and pupils about the acceptable use of mobile technologies, both the school's and personal items that are brought into school.

Our Vision for Computing

Within the RVPLP we will provide a learning environment which provides a range of Computing opportunities and tools. This will empower our children to make relevant and safe choices to support their learning,

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

RVPLP Healthy Schools Ethos- Online Safety

This document should be read in conjunction with the 'Healthy Schools- Online Safety curriculum' document.

- We are mindful about preconceptions- both ours and the children's.
- We believe that teaching a rigorous curriculum around healthy relationships is key to empowering young people to make the right choices- both in the 'real world' and online.
- We aim to protect children from being groomed, sexually exploited or abused online.
- We model and teach what 'healthy relationships' look like.
- We are positive about technology and the children's use of technology.
- We are positive and open to hearing about the children's use of technology so we can **foster an accepting culture in which children are confident that they can talk to us without fear.**

- We do not deal with issues by taking away or 'burying' the use of technology, but rather put measures in place to support a safer use in the future.
- We foster the attitude which communicates to the children that 'even if something happens at home, you can talk to us at school'.
- Teaching staff don't *need* to know about the latest apps or app settings- keeping up would be impossible. We aim to teach a variety of transferable skills, such as how to 'post' politely or which button to press if you feel worried. These skills can be adapted and used on any platform.
- We will further enforce the children's understanding of 'early warning signs' and discuss these feelings in relation to 'real world' and online scenarios.
- This allows children to negotiate all platforms.
- We aim to teach a curriculum which acts as a preventative measure to potential issues, so that we are not *only* reactionary to issues which arise.
- Our two key ideas are 'Awareness' and 'Critical Eyes.'
- We discuss and challenge stereotypes. For example, the term 'stranger'. Looking at previous online safety work many children consider that 'strangers' are old men in hoodies behind computer screens. We challenge and discuss what it means to 'know' someone online. Also that we "know" who we are communicating with because there is a picture and they say so.
- **Technology is not the problem-it's how you use it.'**

Assessing the risks

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities has expanded in all sectors of society bringing young people into contact with a wide variety of influences, some of which may be unsuitable.

The RVPLP recognises that it is important to adopt strategies for the safe and responsible use of the Internet. 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. At a very minimum level of protection, **no child will use the internet without supervision by an adult.**

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

- Methods to identify, assess and minimise risks will be reviewed annually.
- The Executive Headteacher will ensure that the ONLINE Safety & Computing Acceptable Use Policy is implemented and compliance with the policy monitored.

Strategies for the Safe and Responsible Use of the Internet

The school works in partnership with parents, the MCLP, DfES and Montsaye (the school's computer technicians) to ensure systems to protect pupils are reviewed and improved.

- Filtering strategies are selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy provided by Trustnet and selected to suit the age and curriculum requirements of the pupil.
- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- The school's technicians will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Regular
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirements and age of pupils.
- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are not allowed access to social media sites or games sites.
- Newsgroups are not made available to pupils.
- Pupils are not allowed access to public or any chat rooms.

Evaluation of Internet Content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Executive Headteacher or the school's technician. This information will be immediately reported to the Executive Headteacher via a form (Appendix 1).The Executive Headteacher will contact children's parents in relation to the incident.

- Any material that the school believes is illegal must be referred to the Internet Watch Foundation.
- Users must ensure that the use of Internet derived materials complies with copyright law. (Reference Copyright Policy Document)
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Use of Email

The government encourages the use of email as an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits and interesting projects. However, un-regulated email can provide a means of access to a pupil that bypasses the traditional school boundaries. In the school context, therefore, Online mail is not considered private and is monitored by staff, whilst trying to achieve a balance between monitoring that is necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

- Pupils may only use Learning Platform email accounts.
- Pupils must immediately tell a teacher if they receive offensive email and will be encouraged to maintain it as evidence.
- Pupils must not reveal details of themselves or others in email communication, such as address or telephone number, or arrange to meet anyone.
- Pupils may not access home email accounts in school. The school has a high filter level that will block access to hotmail/yahoo etc.
- Email sent to an external organisation is written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- The sending of abusive or inappropriate email messages is forbidden.

Management of Web Site Content

The schools Web Site - www.rothwellschools.org.uk

- The point of contact on the Web Site is the school address, school email and telephone number. Staff or pupils' home information are not to be published.
- Pupils' full names are not to be used on the Web Site, particularly in association with photographs.
- Written permission from parents or carers is obtained before photographs of pupils are published on the school Web Site.

- The Executive Headteacher and nominated Governor take overall editorial responsibility and try to ensure that content is accurate and appropriate.
- The copyright of all material is held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Procedures for Use of Video and Photographs

The school has produced an additional policy in relation to taking photographs in school – Photographic Images Policy

To summarise:
The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in school there is access to:

- Video cameras
- Digital cameras.
- Ipads

Parents are only permitted to photograph their children in public school performances if they have signed a register agreeing to follow the school policy. Parents are not permitted to share images featuring other children on public forums or social media websites.

The sharing of photographs which allow children to be identified via weblogs, forums or any other means on-line will only be allowed with parental consent.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should never be included if the parents/carers have signed a form indicating they do not give permission for their names to be used.

Group photographs are preferable to individual children and young people and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit. Photographs will be centrally stored on the school server.

Both schools will make use their Facebook pages to promote the work of the RVPLP and share information. Any content to be placed on these sites must be agreed with a member of the leadership team before posting.

Video-Conferencing and Webcams

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission will be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school setting. This process should always supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult.

Managing Emerging Internet Applications

Many emerging communications technologies offer the potential to develop new teaching and learning tools. Mobile communications, wide Internet access and multimedia present opportunities need to be evaluated to assess risks, to establish benefits and to develop good practice. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile Phones and Other Emerging Technologies

RVPLP School has considered carefully how the use of mobile technologies can be used as a teaching and learning tool within the curriculum with the following areas of concern to be taken into consideration:

- Cyber bullying - inappropriate or bullying text messages or the videoing of violent or abusive acts
- images or video taken of adults or peers without permission
- Sexting- the sending of suggestive or sexually explicit personal images via mobile phones

As a result of this RVPLP does not allow pupils to bring mobile phones to the school building.

In the case of a request from a parent for their child to bring a mobile phone to school an arrangement where the child leaves their phone with the office staff for the duration of the school day will be made.

(i) Personal mobile devices

Staff are allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children and young people under any circumstances.**

Staff will not use their personal devices in public areas of the school whilst children are present in the building.

Staff are not to connect their personal devices to the school Wireless Network.

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.
- Staff should be aware that games consoles such as the Sony PlayStation, Microsoft Xbox and other such systems have Internet access which may not include filtering. Before use within school, authorisation should be sought from the Executive Headteacher and the activity supervised by a member of staff at all times.
- The school is not responsible for any theft, loss or damage of any personal mobile or computing device.

(ii) School/educational establishment issued electronic and mobile devices

The management of the use of these devices should be similar to those stated above, but with the following additions:

- Where the establishment has provided a mobile device to a member of staff, such as a laptop. Ipad or mobile phone. This equipment should only be used to conduct school business during school hours. If used for personal use outside of school hours the user is responsible for ensuring that the device is not used in a way which could be deemed unacceptable or inappropriate.

School devices will be monitored using NETSUPPORT DNA which will log Keystrokes, pages visited and searches providing a report to the SLT for monitoring purposes.

Devices will be monitored regularly as to their use and appropriate action taken if any unacceptable or inappropriate use is noted or logged through the use of monitoring systems, monitoring software or physical checks.

Regular teaching sessions will be held to ensure that children and young people understand the use of a public domain and the consequences of misuse. Relevant curriculum links will be made to highlight the legal implications and the involvement of law enforcement where appropriate.

Social Networking Advice for Staff

The school has produced an additional policy in relation to staff use of social media - Social Media Policy

To summarise:

Social networking outside of work hours, on non school-issue equipment, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with students outside of Executive Headteacher authorised systems (e.g. school email account for homework purposes)
- Staff should not engage in discussion online with parents that are concerned with the running or organisation of the school.
- Staff should not engage in discussions online with parents regarding any children who attend the RVPLP.
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students)

Authorisation of Internet Access

The school allocates Internet access for staff and pupils on the basis of educational need. Parental permission is required for each pupil.

- The school keeps a record of all staff and pupils who are granted Internet access.
- All pupils accessing the internet on school computers are directly supervised by a member of staff.

- Parents are informed that pupils will be provided with supervised Internet access and are asked to sign and return a consent form to show their understanding and acceptance of the internet rules.

How is the policy introduced to pupils?

- Rules for Internet access are posted in all rooms where computers are used.
- Pupils are informed that Internet use will be monitored.
- Pupils are instructed in responsible and safe use.
- A module on responsible Internet use will be included in the computing scheme of work covering both school and home use, plus within the yearly anti-bullying week.

Staff

- All staff must sign the terms of Online Safety and Computing Acceptable Use' statement.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with a copy of this policy, and are required to sign to show acceptance of the rules.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff are aware that under no circumstances should they be in contact with pupils other than for Executive Headteacher authorised school business.
- The monitoring of Internet use is a sensitive matter. Monitoring procedures are supervised by the Head Teacher and Monsaye leader.

Appropriate and Inappropriate Use by Staff or Adults

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff should receive a copy of this policy and a copy of the Acceptable Use Agreement, which then need to be signed, returned to school or setting to keep under file with a signed copy returned to the member of staff.

This policy will be displayed on the Safeguarding display board as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use. Staff training will underpin the receipt of this policy.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Executive Headteacher immediately and then the Allegations Procedure (Section 12, LSCBN) and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

By Children or Young People:

The Online Safety and Computing Acceptable Use Rules letter for children, young people and parents/carers are outlined in the Appendices. These detail how children and young people are expected to use the internet and other technologies within school or other settings, including downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an email to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

RVPLP will encourage parents/carers to support the rules with their child or young person. This can be shown by signing the Acceptable Use Rules together so that it is clear to the school or setting that the rules are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the internet beyond school.

Further to this, it is expected that parents/carers will adhere to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.
File sharing via email, weblogs or any other means on-line should be appropriate and be copyright free when using the learning platform in or beyond school.

The School Council is actively involved in discussing the acceptable use of technologies and the rules for misusing them.

In the event of inappropriate use:
Should a child or young person be found to misuse the on-line facilities whilst at school the following consequences will occur:

- Any child found to be misusing the internet by not following the Acceptable Use Rules will have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the rules may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.
- A letter will be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing on-line technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Maintaining Computing System Security

The school computing systems will be reviewed regularly with regard to security.

- Virus protection and Firewalls for the whole network are installed and expected to be kept current.
- All portable media, particularly memory sticks, which carry personal school or pupil information are password protected or encrypted for data protection purposes in the event of loss or theft.
- Uploading and downloading of non-approved software is not permitted.
- Homework completed at home may be brought in on CD-ROM or memory stick, but this will have to be virus scanned by the class teacher before use.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet. This is to prevent corruption of data and avoid viruses.
- No programs on disc should be brought in by pupils from home for use in school although staff can seek permission from the Head. This is for both legal and security reasons.
- Unapproved system utilities and executable files are not be allowed in pupils' work areas or attached to Email.
- The schools' technician will ensure that the system has the capacity to take increased traffic caused by Internet use.

How is Parent Support Enlisted?

Internet use in pupils' homes is increasing rapidly, encouraged by offers of free access and continual media coverage. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school can support parents to plan appropriate, supervised use of the Internet at home. Parents are also advised to check if pupils' use elsewhere, such as libraries, is covered by an appropriate use policy.

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school Web Site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents is encouraged.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet is available to parents.

RVPLP will encourage parents/carers to support the rules with their child or young person. This can be shown by signing the Acceptable Use Rules together so that it is clear to the school or setting that the rules are accepted by the child or young person with the support of the

parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the internet beyond school.

Further to this, it is expected that parents/carers will adhere to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File sharing via Email, weblogs or any other means on-line should be appropriate and be copyright free when using the learning platform in or beyond school.

The School Council is actively involved in discussing the acceptable use of technologies and the rules for misusing them.

In the event of inappropriate use:

Should a child or young person be found to misuse the on-line facilities whilst at school the following consequences will occur:

- Any child found to be misusing the internet by not following the Acceptable Use Rules will have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the rules may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.
- A letter will be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing on-line technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Appendix 1
Unsuitable Website Reporting Form

Name of reporting adult	
Date:	
Address of website:	
Details of access: (where and when the website was accessed; nature of the site; name of children who accessed the site)	
Actions by the Executive Headteacher:	

Pupil Online Safety and Computing Acceptable Use Rules Key Stage 2

This is to be read through with your child and then signed. Your child will be allowed Internet Access after this is returned to school.

At RVPLP, we expect all children to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

- Children using the Internet are expected not to deliberately seek out offensive materials. Should any children encounter any such material accidentally, they are expected to report it immediately to a teacher.
- Children are expected not to use any inappropriate language in their email communications and contact only people they know or those the teacher has approved.
- Children must ask permission before accessing the Internet and must only access it under the supervision of staff.
- Children should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet.
- No programs on memory stick or CD Rom should be brought in from home for use in school.
- Homework completed at home may be brought in on CD-ROM or memory stick, but this will have to be virus scanned by the class teacher before use.
- Personal printing is not allowed on our network for cost reasons (e.g. pictures of pop groups/cartoon characters).
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Children consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.

I have read through this agreement with my child and agree with the content.

Signed:
(Parent/Responsible Adult)~~)~~ _____

Pupil OnlineSafety and Computing Acceptable Use Rules Key Stage 1 & EYFS

This is to be read through with your child and then signed. Your child will then be allowed Internet Access after this is returned to school.

At RVPLP, we expect all children to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

Our Internet Rules

- We will use the internet safely to help us to learn.
- We only use the programs chosen by our teachers.
- We know have to ask for help if we see something on the internet that we do not like or something that upsets us.
- We are able to look after each other by using the internet safely.
- We can go to www.thinkuknow.co.uk for help.
- We know that it is important to follow the rules.

I have read through this agreement with my child and agree with the content.

Signed: _____
(Parent/Responsible Adult)

RVPLP School Staff Online Safety and Computing Acceptable Use Policy & Social Media Policy Agreement

I have read and understood the contents of the Rothwell Victoria Primary Learning Partnership's Social Media Policy and Online Safety and Computing Acceptable Use Policy and will comply with their requirements during my employment with the Rothwell Victoria Primary Learning Partnership. I am fully aware of and accept that the Rothwell Victoria Primary Learning Partnership reserves the right, in accordance with these Policies, to monitor internet usage and take appropriate action for non-compliance of this policy.

Signed_____

Print_____

Date_____