ROCKMOUNT PRIMARY SCHOOL

Online Safety Policy/Acceptable Use Agreements

September 2025 Review: September 2026

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, visitors and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also considers the National Curriculum computing programmes of study.

3. Roles and Responsibilities

3.1 The Governing Board

The Governing Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Governing Board will co-ordinate meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding leads (DSLs). Governors should ensure that they are well informed about the annual review of the school IT filtering and monitoring systems to check their effectiveness and ensure that the school leadership team are aware of what provision is in place and how to escalate any concerns.

The governor who oversees online safety is **Richard Steward**

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet **(Appendix 3)**

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Leads (DSLs)

Details of the school's DSLs are set out in our Safeguarding Policy as well as relevant job descriptions.

The DSLs take lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, Computing Subject Leader and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged **(on CPOMS or Appendix 5)** and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy
- Updating and delivering staff training on online safety (**Appendix 4** contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing reports on online safety in school to the headteacher and/or Governing Board as and when required

This list is not intended to be exhaustive.

3.4 The Computing Subject Leader

The Computing Subject Lead is responsible for:

- On-site liaison regarding local authority applied filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Working with external technicians to ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Directing technicians to attend to online safety concerns and tasks requiring action using the engineers' task sheet; follow-up to ensure tasks have been satisfactorily completed
- Flagging up potentially dangerous sites for blocking and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged using CPOMs or Appendix 5 and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy
- This list is not intended to be exhaustive.

3.5 All staff and visitors

All staff, including contractors and agency staff, and visitors are responsible for:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (**Appendix 3)** and ensuring that pupils follow the school's terms on acceptable use **(Appendix 1 (EYFS/KS1) and Appendix 2 (KS2))**
- Working with the DSLs to ensure that any online safety incidents are logged **(Appendix 5)** and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy
- Encouraging pupils to come forward if they discover inappropriate content being accessed (such as left over on a device from a previous user's session) and making clear that they will not be in trouble themselves for reporting it.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment both online and offline and maintaining an attitude 'this could happen here'
- This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents and carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet **(Appendices 1 and 2)**
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use our systems, such as Google Classroom, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Parents/Carers can seek further guidance in **Appendix 7**

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use **(Appendix 3).**

3.7 All pupils (at a level that is appropriate to their individual age and ability)

Pupils are expected to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught 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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online and including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

5. Educating Parents/Carers about Online Safety

The school will raise parent/carer awareness of internet safety in letters or other communications home and in information via the website and/or Google Classroom. This policy will also be shared with parents and carers.

Online safety may also be covered during parent/carer evenings and other parent/carer events or meetings.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher, the DSLs and/or the Computing Subject Lead.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff will discuss cyber-bullying with their classes.

Staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and visitors (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also supplies information on cyber-bullying to parents and carers so that they will be more aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSLs will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices (and any back-up copies created), including mobile phones, iPads and other tablet devices, where they believe there is a good reason to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules
- The pupil and/or the parent refuses to delete the material themselves

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSLs or other members of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), or
- Make a copy of that material as evidence (of a criminal offence or a breach of school discipline) before deleting it, and/or
- Report it to the police

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure, as laid out in the school Complaints Policy.

7. Acceptable Use of the Internet in School

All pupils, parents/carers, staff, visitors and governors are expected to comply with the school's policy regarding the acceptable use of the school's ICT systems and the internet **(Appendices 1-3).** Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

Websites visited by pupils, staff, visitors, governors (where relevant) may be monitored and/or blocked to ensure compliance with the above.

More information is set out in the acceptable use agreements **(Appendices 1, 2 and 3)**

All classrooms will display 'SMART' rules as a reminder of how we can use the internet safely. **(Appendix 6)**

8. Pupils Using Mobile Devices in School

As part of our ongoing commitment to fostering a positive and healthy learning environment, **Rockmount Primary School is a 'smartphone free' school.**

While technology offers numerous benefits and opportunities, recent research has highlighted a concerning link between the age at which a child gets their first smartphone and mental health issues in young adulthood.

(see research https://sapienlabs.org/wp-content/uploads/2023/05/Sapien-Labs-Age-of-First-Smartphone-and-Mental-Wellbeing-Outcomes.pdf)

Some parents choose to provide their children with phones once they start walking to school independently, primarily for safety reasons. Parents who feel the need for their child to have a phone for safety reasons are recommended to consider pay-as-you-go basic phones without internet access. These phones are both affordable and readily available.

Children from Nursery to Year 4 are **not** permitted to have phones in school.

Year 5 and Year 6 pupils who make their own way to and from school (when parents/carers have signed a permission form) are **not** allowed to bring in smartphones but may use a basic phone without internet access. Pupils are still required to hand in a phone at the beginning of each school day.

More detailed information and resources are available at the Smartphone Free Childhood website.

Smartphone Free Childhood

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school Behaviour Policy, which may result in the confiscation of their device.

9. Using School-supplied Devices Outside School

All staff members and children/parents/carers will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping in place the password-protection which has been set up on the device – passwords should not be changed without prior agreement
- Leaving security settings intact to ensure that the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Not modifying anti-virus and anti-spyware software which is installed, and allowing updates to run when prompted
- Returning the device to the school premises at appropriate intervals to ensure that the latest operating updates are applied
- Only logging in to devices using school-supplied log-ins, not personal accounts
- Logging out of resources which require a user account to use (such as Google Classroom or Times Tables Rock Stars) after each session. Avoid selecting "save password/remember me" type options when using a shared school device.

Staff members must not use the device in any way which would violate the school's terms of acceptable use **(Appendix 3).**

Staff members using personal devices at home for work purposes should ensure their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, in the first instance they should seek advice from the Computing Subject Leader.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our school Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct. The actions taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive, as part of their safeguarding training, information on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training as and when required/appropriate, as well as relevant updates (for example through emails, inset days and staff meetings).

The DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Visitors will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding Policy.

12. Monitoring Arrangements including Filtering and Monitoring

The school will log behaviour and safeguarding issues related to online safety. An incident report log can be found on CPOMs or **Appendix 5.**

Appropriate filtering and monitoring

In line with the guidance in 'Keeping Children Safe in Education,' we use the London Grid for Learning (LGFL) to filter and block access to inappropriate websites. Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system, which is made specifically to protect children in schools.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)

2. Internet and web access

3. Active/Pro-active technology monitoring services

At Rockmount, we use Physical Monitoring. London Grid for Learning provides a technology-based monitoring system that actively monitors use through keywords and other indicators across devices. This system is particularly effective at drawing attention to concerning behaviours, communications or access.

13. Links with Other Policies

This online safety policy is linked to our:

- Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct/disciplinary procedures
- Data Protection Policy
- Complaints Policy and Procedure
- Antibullying Policy
- Mobile Phone Statement

This policy will be reviewed every two years by the Headteacher and/or a member of the Senior Leadership Team. At every review, the policy will be shared with the Governing Board.

Appendix 1: EYFS and KS1 Acceptable Use Agreement (pupils and parents/carers)

(To be completed as part of the application and induction pack/process)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• I will be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
• Not use my school Google Classroom or Google Meet account for activities which are not part of my lessons and learning
I agree that the school will monitor the websites I visit and that there will be consequences from our Behaviour Policy if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 Acceptable Use Agreement (pupils and parents/carers)

To be completed as part of the application and induction pack/process for children new to the school.

All KS2 classes will sign an A3 whole class copy of this acceptable Use agreement which will be kept in the class behaviour folder.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Use my school Google Classroom or Google Meet account for personal communications which are not part of my lessons and/or learning, either in school or remotely

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 3: Acceptable Use Agreement (staff, governors and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VISITORS/VOLUNTEERS

The Acceptable Use Policy is intended to ensure that staff and volunteers will be responsible users and stay safe whilst using the internet and other communication technologies for educational, personal and recreational use. This covers the use of digital technologies in Rockmount Primary School including **email, Internet, intranet and network resources,** learning platform, software**, equipment and systems.**

- I will only use Rockmount Primary School's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the school.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access any of the Rockmount systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with Rockmount's Data Protection Policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I understand that my personal online communication tools must not be used with pupils or parent/ carers and will not communicate or 'befriend' any pupil or parent/care using such methods.
- I will only use the approved email system for any email communication related to work at Rockmount Primary School. This is currently: LGFL staffmail.
- I will only communicate with pupils and/or parent/carers using official school systems.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will immediately report any damage or faults involving equipment or software.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Online Safety Lead (if by a child) or Headteacher (if by an adult).
- I will not download any software or resources from the Internet that can compromise the network or are not adequately licensed.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings without permission.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software. I will keep any 'loaned' equipment up-to-date, using Rockmount recommended anti-virus, firewall and other ICT 'defence' systems.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/ video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name or other personal information, those who are featured.

- I will ensure that any private social networking sites / blogs etc that I create, or actively contribute to, are not confused with my professional role. I understand that it is my responsibility to ensure I know how to use any such tools so that I do not compromise my professional role, such as setting appropriate security settings.
- I will not create a business account on any social networking site unless in full agreement with the appropriate manager, agreed for specific circumstances.
- I agree and accept that any computer, laptop or tablet loaned to me by Rockmount is provided solely to support my professional responsibilities and that I will notify them of any “significant personal use” as defined by HM Revenue & Customs.
- I will access Rockmount’s resources remotely (such as from home) only through approved methods and follow e-security protocols to access and interact with those materials.
- I will only transport, hold, disclose or share personal information about myself or others as outlined in Rockmount’s Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be password protected. Paper based protected and restricted data must be held in lockable storage.
- I understand that it is my duty to support a whole organisation safeguarding approach and I will alert Rockmount’s Designated Safeguard Lead or relevant senior member of staff if I feel the behaviour of any service user or member of staff may be a cause for concern or inappropriate.
- I understand that the data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I understand that all Internet usage and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.
- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

User Signature

I agree to abide by all the points on this Acceptable Use Policy

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand Rockmount’s most recent E-Safety and Data Protection Policies.

Signed:	**Date:**

Appendix 4: Online Safety Training Needs – Self Audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/visitor:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person/s holding lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the main details of the school's acceptable use agreement for pupils, parents, staff, visitors and governors?	
Do you know what steps to take if misuse is found to have occurred on a school device?	
Do you change your password for accessing the school's ICT systems whenever you are prompted?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: Rockmount Primary School Online Safety Incident Report

CPOMS MAY ALSO BE USED TO LOG ANY CONCERN

Name and role of person reporting incident:						
Date incident was logged:						
Where did the incident take place:	**Inside school?**			**Outside school?**		
Date of incident(s):						
Time of incident(s):						
Reported to: (tick)	**Class Teacher**	**Computing Leader**	**Headteacher / SLT**	**DSL**	**Parent/ Carer**	**Other**

Who was involved in the incident(s)?	**Full names and/or contact details**
Children/young people	
Staff member(s)	
Parent(s)/Carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		**Accessing someone else's account without permission**	
Forwarding/spreading chain messages or threatening material		**Posting images without permission of all involved**	
Online bullying or harassment (cyber bullying)		**Posting material that will bring an individual or the school into disrepute**	
Racist, sexist, homophobic, religious or other hate material		**Online gambling**	
Sexting/Child abuse images		**Deliberately bypassing security**	
Grooming		**Hacking or spreading viruses**	
Accessing, sharing or creating pornographic images and media		**Accessing and/or sharing terrorist material**	
Accessing, sharing or creating violent images and media		**Drug/bomb making material**	
Creating an account in someone		**Breaching copyright regulations**	

else's name to bring them into disrepute			
Other breach of acceptable use agreement, please specify			

Full description of the incident including any evidence collected and the name of all social media involved.	
What action has been taken:	
Follow up action/ review date (if required):	

The completed form must be passed to a member of SLT. The incident must be added to the log maintained at the front of the Incident Folder and this Online Safety Incident Report Form must be placed in the relevant section of the folder.	
Signed: **(member of staff reporting incident)**	**Signed:** **(member of SLT)**

Appendix 6: SMART Rules

Appendix 7: Further guidance for parents

CEOP:

www.thinkuknow.co.uk

www.ceop.police.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety

UK Safer Internet Centre: www.saferinternet.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Report Harmful Content: https://reportharmfulcontent.com/

360 Safe Self-Review tool for schools: www.360safe.org.uk

Childnet: www.childnet.com

Step Up Speak Up – Online Sexual Harassment Guidance:

www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals

Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools

Internet Matters: www.internetmatters.org

Parent Zone: https://parentzone.org.uk

Parent Info: https://parentinfo.org

NSPCC: www.nspcc.org.uk/onlinesafety

ChildLine: www.childline.org.uk

Net Aware: www.net-aware.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

Action Fraud: www.actionfraud.police.uk

Get Safe Online: www.getsafeonline.org