The Roebuck School

On-line Safety policy



# Written on behalf of the staff

# by Mrs Alexander-Steele

Reviewed: Sept 2020

|  |
| --- |
| **Responsibilities for the Policy** |

|  |  |
| --- | --- |
| **Online Safety lead:** | Jill Alexander-Steele |
| **Computing subject leader:** | Robert Duck |
| **Link Governor:** | Tanya Honey |
| **Policy to be read and adhered to by:** | All staff in school  All Governors |

|  |
| --- |
| **Aims of this policy** |

The purpose of this policy is to:

* Ensure that key expectations of all members of The Roebuck School community are clear and understood with respect to the use of IT based technologies.
* Safeguard and protect children and staff.
* Ensure that all school staff are fully trained and aware of how they can work with children and be safe and responsible with the internet and other IT and communication devices.
* Establish clear expectations and codes of conduct relevant to responsible use of the internet for educational, personal or recreational use.
* Have clear structures to deal with online abuse, such as online bullying.
* Ensure all members of the school community understand appropriate and inappropriate use of the internet, IT and other communication devices.

# **Communication of the Policy**

The policy will be communicated in the following ways:

* Posted on the school website.
* Part of induction for new staff.
* Regular updates and training for all staff.
* Acceptable use agreements discussed with staff and pupils. Acceptable use agreements will be issued to the whole school community on entry to the school, including mid-year transfers and at Reception class induction.

**Linked Policies**

It is important that this policy is read in conjunction with the following policies:

* Staff Conduct
* GDPR
* Safeguarding and Child Protection
* Anti-Bullying
* Computing

|  |
| --- |
| **Rationale** |

At The Roebuck School, we believe that, as we live in an increasingly technological society, we need to prepare children to live and work in that environment. Whilst exciting and beneficial to children’s lives within education and their lives beyond school, technology, particularly web-based resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these technologies. At The Roebuck School, we understand the responsibility to educate our pupils on Online Safeguarding issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. In addition to creating safe and responsible internet users, we are also committed to ensuring our safeguarding practice is of the highest standard to ensure children’s safety and wellbeing. It is also important to recognise the constant and fast paced evolution of technology within our society as a whole. Currently, the internet technologies children are using, both inside and outside of the classroom, include:

* Websites
* Learning Platforms and Virtual Learning Environments
* Email and Instant Messaging
* Chat Rooms and Social Networking
* Blogs and Wikis
* Podcasting
* Video Broadcasting
* Music Downloading
* Gaming
* Mobile/ Smart phones with text, video and/ or web functionality
* Other mobile devices with web functionality
* APPs

This list is not exhaustive and, as technology continues to develop, will be ever-evolving and will be amended with each policy review.

Both this policy and the Acceptable Use Agreement (for all staff, Governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc.) and include the use of external / personal devices whilst on school premises. Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will, however, endeavour to add any important issues to the policy on our website.

The main areas of risk for The Roebuck School’s community are:

**Content –** inappropriate content, extremist content, lifestyle websites promoting harmful behaviours, reliability of content.

**Contact –** adults understand the boundaries of appropriate online contact, peer-on-peer cyber bullying, online grooming, security and password sharing, inappropriate communication with unfamiliar people, e.g. through social media, gaming, etc.

**Conduct –** knowing when and how to report inappropriate activity, awareness of what inappropriate searches are and the reasons for not carrying them out, digital footprint and online reputation, health and wellbeing – effects of periods of time spent online, influence of websites, e.g. body image, sexting, copyright.

**Commerce -** R**isks such as online gambling, inappropriate advertising, phishing and or financial scams’. (New in KCSiE 2021)**

# **Roles and Responsibilities**

As Online Safeguarding is an important aspect of strategic leadership within the school, the Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the Head Teacher and Online Safety Champion to keep abreast of current issues and guidance through organisations such as LGfL, Becta, CEOP (Child Exploitation and Online Protection) and Childnet. The Governors are updated by the Head Teacher and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school’s Acceptable Use Policy (signed agreements) for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the 3 following mandatory school policies: safeguarding and child protection, health and safety, and behaviour (including anti-bullying).

# **Online Safeguarding Development for Staff**

Our staff receive timely information and training on Online Safeguarding issues in the form of staff meetings and notices. New staff receive information on the school’s acceptable use policy as part of their induction. All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safeguarding and know what to do in the event of misuse of technology by any member of the school community. All staff are encouraged to incorporate Online Safeguarding activities and awareness within their curriculum areas. We endeavour to embed Online Safeguarding messages across the curriculum whenever the internet and/or related technologies are used. The Online Safeguarding policy will be introduced to the pupils at the start of each school year.

It is the expectation that staff model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging off, research skills, awareness of copyright, etc. All staff are expected to log off/lock devices when they have finished working or are leaving the computer unattended.

# **Online Safeguarding in the Curriculum**

The school provides opportunities within a range of curriculum areas to teach about Online Safeguarding. Educating pupils on the dangers of technologies that maybe encountered outside school is done formally when opportunities arise and as part of the Online Safeguarding/Computing curriculum. Older pupils will be made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them. Pupils in upper Key Stage 2 are also taught about copyright and respecting other people’s information, images, etc through discussion, modelling and activities.

Older pupils are made aware of the impact of online bullying and will know how to seek help if they are affected by these issues. Pupils will also be aware of where to seek advice or help if they experience problems when using the internet and related technologies, e.g. parent/carer, teacher/ trusted staff member or an organisation such as Childline/ CEOP report abuse button. Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

All users, including pupils, read and sign an Acceptable Use Agreement to demonstrate that they have understood the school’s Online Safeguarding Policy. Pupils are not allowed to deliberately access on-line materials or files on the school network of their peers, teachers or others. Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks. It is made clear that pupils should never be allowed to log on or use teacher and staff logins.

# **Parental Involvement in Online Safety**

It is the role and responsibility of parents to monitor children’s online safety at home. School offers Online Safeguarding information through:

* Workshops provided by Lancashire County Council representatives.
* Internal workshops/information sessions.
* Information and guidance on current and relevant issues regarding online safety, e.g. risks and threats.
* Acceptable user agreements will be sent home annually and parents will be expected to share these with their children and return a signed copy to confirm that they have done this.

# **Implementation of the policy**

The Roebuck School is aware of its responsibility when monitoring staff communication under current legislation and takes into account: Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998. It is the policy of the school that children will not be permitted to access the Internet without the direct supervision of a teacher or other responsible adult. The Lightspeed filtering system, provided by Lancashire County Council (LCC), is designed to restrict access to unsuitable sites. Any changes to the filtering policy are logged and only available to staff with the approved ‘web filtering management status.’ The school ensures network health through the use of Sophos anti-virus software (from LCC). Staff will endeavour to monitor all sites the children reach and protect the anonymity of all pupils using the Internet at school.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required. The school does not allow pupils access to internet logs. If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher and then to the Head Teacher. It is the responsibility of the school to ensure that anti-virus protection is installed on all school machines. This automatically updates.

Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school’s responsibility to install or maintain virus protection on personal systems. Pupils and staff are not permitted to download programs or files on school based technologies. If there are any issues related to viruses or anti-virus software, the Head Teacher should be informed.

# **Data Security**

The accessing of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. Staff use encrypted devices or secure remote access when they need to access sensitive or personal data off-site, e.g. password protected pen drives, etc. All personal data is only accessed at school by selected members of staff and, unless there is an emergency, this would not be accessed outside of school. Storage of data in school is in-line with the school’s GDPR procedures.

School requires the Technical Support Provider (Western) to be up-to-date with LCC services and school policies.

# **Managing the Internet**

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Lancashire Grid for Learning (LGfL) is logged and the logs can be randomly but regularly monitored. Whenever any inappropriate use is detected, it will be followed up. The school allows pupils to have supervised access to Internet resources (where reasonable) through the school’s fixed and mobile internet technology. Staff will preview any recommended sites before use. Raw image searches with pupils should be conducted on age-appropriate (pupil friendly) search engines, e.g. Kiddle. If Internet research is set for homework, it is advised that parents check the sites and supervise the work. Parents will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources. All users must observe copyright of materials from electronic resources.

# **Portable Technologies**

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones and watches are familiar to children outside of school too. They often provide a collaborative, well known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

# **Personal Mobile Devices**

The school allows staff to bring in personal mobile phones and devices for their own use. During working hours, these should be stored securely and must not be accessed in the presence of children. The school is not responsible for the loss, damage or theft of any personal mobile device. The use of personal mobile phones and devices to take photographs of children or access personal data is strictly prohibited.

Visitors, including parents, to the school are required to keep their mobile devices securely in their personal property and should not remove them from their bags or pockets. This is explained to all visitors when they arrive at school.

# **School-Owned Mobile Devices**

The school has a mobile phone which staff can use when they take pupils off the school site. Where the school provides a laptop or iPad for staff, only these devices may be used to conduct school business outside of school and should not be used by anyone other than the member of staff that they are assigned to. The sending of inappropriate messages between any members of the school community is not allowed.

# **Managing Email**

The use of email within most schools is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or international.

The school gives all staff and governors (and the Clerk to the Governing Body) their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, email histories can be traced. This should be the account that is used for all school business. Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper. Staff sending emails to external organisations, parents or pupils are advised to cc. the Head Teacher. All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette), particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication. Staff must inform the Head Teacher if they receive an offensive e-mail.

# **Safe Use of Images**

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils. These images should only be taken on school devices, unless otherwise approved by the Head Teacher, e.g. residential trips where wifi access is not available for the uploading of images. In such circumstances, staff are aware that these images should be shared only on school sites, e.g. school website, school Twitter account, ClassDojo, etc. and must be destroyed at the earliest opportunity and removed from any ‘cloud’ backup.

# **Publishing Pupils’ Images and Work**

On a child’s entry to the school, all Parent/Carer(s) will be asked to give permission to use their child's work/photos in the following ways: on the school website, in the school prospectus and other printed publications that the school may produce for promotional purposes, recorded/ transmitted on a video or webcam, in display material that may be used in the school’s communal areas, display material that may be used in external areas (i.e. exhibition promoting the school), general media appearances (e.g. local/ national media/ press releases sent to the press highlighting an activity). This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child’s circumstances where consent could be an issue, e.g. divorce of parents, custody issues. Parent/Carer(s) may withdraw permission, in writing, at any time. Pupils’ surnames will not be published alongside their image. E-mail and postal addresses of pupils will not be published.

Visitors to the school, including Parent/Carer(s) are not permitted to record or capture any images of children, including during performances. After performances, Parent/Carer(s) will be given opportunity to take a photograph of their own child with the clear expectation that it will not contain any other children. This is to safeguard against the publishing of children on social media sites. On some occasions, school may take photographs of individual/groups of children, which may be offered to parents on the understanding that these will not be published on social media or any other online platforms.

# **Storage of Images**

For the purpose of safeguarding staff and children, all school-owned laptops and handheld devices must not be taken home with children’s photographs or personal data stored on their hard drives. Staff must also ensure that they do not have any children’s photographs or personal data stored on their personal removable media. If school-owned technologies are used to take photographs of children during school hours or on a school trip, these should be downloaded onto the secure ‘Teacher’ drive on the school network and deleted from the portable device. These portable devices should not be taken off school premises before the photographs have been removed.

# **Webcams and CCTV**

We do not use publicly accessible webcams in school. Webcams in school would only ever be used for specific learning purposes, e.g. monitoring hens’ eggs, and never using images of children or adults. Misuse of the webcam by any member of the school community will result in sanctions.

# **Misuse and Infringements**

Complaints and concerns relating to Online Safeguarding should be reported to the Head Teacher. Incidents and infringements should be logged. Any complaints or concerns regarding the Head Teacher should be reported to the School’s Chair of Governors. Please see Whistle Blowing Policy for more information.

# **Inappropriate Material**

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Head Teacher/Online Safeguarding Co-ordinator. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Head Teacher/Online Safeguarding Co-ordinator. Depending on the seriousness of the offence and investigation by the Head Teacher/Local Authority, support may be sought from other agencies, i.e. UK Safer Internet Centre helpline, CEOP, PREVENT officer. If deemed of a serious nature, immediate suspension, possibly leading to dismissal, and involvement of police are all possible consequences. Parents/carers will be informed of specific online safety incidents which involve pupils for whom they are responsible.

# **Equal Opportunities Pupils with additional needs**

The school endeavours to create a consistent message with parents for all pupils and this, in turn, should aid the establishment and future development of the schools’ Online Safeguarding rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safeguarding issues. Internet activities are planned and well managed for these children.

Parent/Carer(s) are asked to read through and sign acceptable use agreements on behalf of their child on admission to school. Parent/Carer(s) are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (eg on the school website). The school disseminates information to parents relating to Online Safeguarding where appropriate in newsletter items.

# **Writing and Reviewing this Policy**

This policy will be reviewed every 24 months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

|  |
| --- |
| **Reviewing the policy** |

POLICY REVIEW:

This policy will be reviewed every year by the Head Teacher and Online Safety Champion.

Date reviewed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Headteacher)

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Chair of Governor’s committee)

Signed copy in school