Redesdale Primary School

Online Safety & Acceptable Usage Policy

Adopted by Sub Comm:	November 2023
Policy review date:	November 2024

Redesdale Primary School

Online Safety & Acceptable Usage Policy

Introduction

At Redesdale Primary School we understand the responsibility we have to educate our children regarding staying safe online; teaching them 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.

Online Safety encompasses Internet technologies and electronic communications such as mobile phones, tablets, and games consoles. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Redesdale Primary School has a whole school approach to the safe use of ICT and creating a safe learning environment includes three main elements:

- Responsible ICT use by **ALL** (staff, children, parents/carers, volunteers, and visitors); encouraged by education and made explicit through school policies.
- A comprehensive online safety programme for **ALL**.
- Safe and secure Internet access including the effective management of filtering systems.

This policy is to be read in conjunction with the Safeguarding and Child Protection Policy, Social Networking Policy, Cyber-Bullying Policy, Remote Learning Policy and Remote Learning Plan.

School Responsibilities

The implementation of this policy should be carried out so that all staff are familiar with the school's policy including:

- safe use of email
- safe use of the Internet
- safe use of the school network, equipment, and data
- safe use when joining meetings online and providing remote learning for pupils during any instances of disruption
- safe use of digital images and mobile devices, such as mobile phones and iPads.
- publication of children's information/photographs on the school website and on other platforms such as X (formerly Twitter).
- procedures in the event of misuse of technology by any member of the school community.
- their role in providing online safety education for children.
- Understanding their responsibilities regarding filtering and monitoring.

Staff are reminded/updated about online safety regularly and new staff receive information on the school's **Online Safety & Acceptable Usage Policy** as part of their induction. Staff must sign an **'Authorised Users Agreement' and 'Staff Information Systems Code of Conduct,** before using the Internet, mobile devices or systems in school **(see Appendix A(i), A(ii) and A(iii) – 'Staff Online Safety & Acceptable Usage'**).

In managing the school online safety: -

- Online safety messages are embedded across the curriculum as part of our Computing & PSHE curriculum.
- All staff will undergo safeguarding and child protection training; including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring at induction. The training should be regularly updated. Induction and training should be in line with any advice from local safeguarding partners.
- The four areas of risk will be taken into consideration;
    - **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
    - **Contact:** being subjected to harmful online interaction with other users; for example, peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
    - **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
    - **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)
      (Keeping Children Safe in Education 2023 & Meeting Digital and Technology Standards in Schools & Colleges 2023)

Why Internet Use is Important

The Internet is an essential element in 21st century life for education, business, and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. As Redesdale Primary School continues to embed the use of iPads for our children, teaching children to access the internet responsibly and safely becomes an essential part of pupils' education.

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and

extend learning activities across the curriculum. Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation.

Pupils will be taught how to evaluate Internet content

If staff or children discover unsuitable sites, the URL (address), details of content (captured using screenshots or school iPad images) and type of device must be reported as soon as possible to the school ICT Subject Leader/ Deputy Headteacher. Staff should ensure that the use of Internet derived materials by staff and by children complies with copyright law. Children should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Curriculum

The Internet and online resources are increasingly used across the curriculum. We believe it is essential for online safety guidance to be given to the children on a regular and meaningful basis. The use of new technologies for pupils to engage with staff safely and securely during remote learning has prompted an increased focus on staying safe online and we continually look for new ways to promote online safety.

- We provide opportunities within a range of curriculum areas to teach about online safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and explicitly as part of the Computing curriculum. This is covered using the Common-Sense Media Digital Citizenship programme which is built into our curriculum across Y1-Y6.
- Children are taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the Computing curriculum.
- Children are aware of the impact of online bullying through PSHE and Computing lessons and know how to seek help if they are affected by these issues. Children are also aware of where to seek advice or help if they experience problems when using the internet and mobile devices.
- Children are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.
- We engage with Northumbria Police to involve PCSO led online safety presentations to reinforce our message to pupils.
- We ensure that pupils engaging in remote learning do so safely and securely, adhering to our Pupil Acceptable Use Policy.
- We ensure that remote learning devices loaned to families during remote learning are safe to use and have the appropriate restrictions built-in, for example, apps can only be installed remotely by school IT admin; age-restrictions are applied to each device to prevent access to inappropriate content.

Electronic Mail (Email)

Children will only have access to their own Redesdale Primary School Office 365 account when logging onto the local network within school . This account is also used outside of school when appropriate and provides pupils across Key Stage 2 with access to Microsoft Teams, our preferred platform for remote learning. They are not allowed access to personal email accounts whilst in school. Children must immediately tell a teacher if they receive an offensive email. It is vitally important that children must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission. Emails sent to an external organisation should be written carefully in the same way as a letter written on school headed paper. Emails should never be used to send or forward chain letters or any material which may contravene school policies (e.g., jokes, pictures of a racist or sexist nature).

School Website & X(formerly Twitter)

The website and X(formerly Twitter) account must be updated regularly with information from each phase, subject and whole school events. Permission must be obtained from all people who will appear in a photograph or video before the footage is recorded (**see Appendix B(ii) – 'Media Consent Form'**). Remember that consent is also required from the school staff and parents and any other adults who may appear on the image. The school should not display images of children or staff on the website without such consent and contact details should not include any personal information regarding children, staff, governors, or parents.

Mobile phones

Staff and governors should only use their personal mobile phones or devices with the **direct permission** of the Headteacher if/when:

- It is on silent mode
- Within school for personal use when children are not present
- Making personal calls in private, i.e. not in public areas of school, classrooms or corridors.
- In children's presence in an emergency or on a school trip when communicating with school or with travel providers.
- In children's presence in an emergency or on a school trip or sporting event for taking images, videos of the pupils during the event:
    - Any images or videos taken should be immediately transferred to a member of staff's iPad upon return to school and permanently deleted from their personal device, including from the 'recently deleted folder'.

  Using for a specific lesson or demonstration on mobile phone safety.

Parents, carers, and visitors **should not** use mobiles phones in school at any time. Mobile phones **should not** be used around the school when children are present – except in an emergency.
The Headteacher, Deputy Headteacher, Assistant Headteacher, Caretaker and School Business Manager are the only staff who are allowed to use their mobile phones or devices around school for work purposes on a daily basis.

Redesdale Primary School does not encourage children to have mobile phones in school. If a Year 5 or 6 parent wishes their child to have a mobile phone in case of an emergency and because they are travelling to and from school on their own, they must complete a 'Mobile Phone Online Safety Agreement' and ensure both they and their children are aware of the rules and policies which they must follow. (See **Appendix E** – '**Mobile Phone Online Safety Agreement and Rules'**). This agreement is also available in Office Form format, all information obtained from parents is stored securely in the cloud.

Social Networking Sites

It is advised that all staff uphold the law and maintain a good standard of behaviour both inside and outside of school; both online and offline. The content in cyberspace does not elude the law – a posting in the public domain can still constitute a defamatory publication. Staff must read this policy in conjunction with our **Social Networking Policy.**

By adhering to our **Social Networking Policy** staff are not only protecting the reputation of the school but also their own reputation and chances for future employment.

Online Safety Complaints/Incidents

As a school we take all precautions to always ensure online safety. However, due to the international scale and linked nature of internet content, the availability of mobile devices and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device. The school cannot accept liability for material accessed or any consequences of this. Complaints of Internet misuse will be dealt with firstly by the Class Teacher, then by the Computing Subject Leader or the Deputy Headteacher/Headteacher.

It is important that the school work in partnership with children and parents to educate them about cyber-bullying and filtering and blocking harmful and inappropriate content; children, staff and families need to know what to do if they or anyone they know are a victim of cyber-bullying or harmful and inappropriate content. All bullying and safeguarding incidents should be recorded and investigated.

All parents receive an '**Online Safety Rules'** letter which they must sign (**Appendix C**) along with the '**Pupil Online Safety & Acceptable Usage Policy' (Appendix D(i))** and agreements and rules (**Appendix D(ii) and D(iii) – Foundation Stage & KS1 and KS2**). Additionally, Year 5 and 6 pupils receive a **'Mobile Phone Online Safety Agreement and Rules'** letter for parents to sign **(Appendix E**). This agreement is also available in Office Form format, all information obtained from parents is stored securely in the cloud.

Reviewing this Policy

This policy will be reviewed annually as the Internet and the use of mobile devices in school develop. If you have any comments about this policy, please pass them onto the Deputy Headteacher or Computing Subject Leader.

Appendix A(i) **REDESDALE PRIMARY SCHOOL**

Staff Online Safety & Acceptable Usage

Introduction

Redesdale Primary School has a whole school approach to the safe use of Information and Communication Technology (ICT), and it sets out the terms and conditions under which users will:

- Access the Internet
- Make use of resources/information on the Internet
- Disseminate information arising out of the Internet
- Disseminate information via the Internet
- Communicate using the Internet
- Understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

This applies to all staff, to whom the Internet is available via both networked and stand-alone PC's or mobile devices within school with access to the Internet.

Home working has become more prevalent as part of 'remote learning' where staff have spent time working from home and delivering teaching online from home. When staff are working from home and using their own Internet provider, it is expected that they log on to their secure school Office 365 account to access their school resources. All resources pertaining to school should be stored on their school Microsoft OneDrive space and / or the school Microsoft SharePoint space for staff to access.

If at any point, staff are required to revert to remote education for whole groups of children and deliver live lessons via Microsoft Teams from home, there is no requirement for them to use a camera. When joining school-related meetings from home which require cameras to be on, staff should ensure that they are professionally dressed, and their background screens don't reveal any personal information or details. This can often be easily blurred using Microsoft Teams background technology.

This information is to be read in conjunction with the school **Safeguarding and Child Protection Policy**, **Social Networking Policy**, **Remote Learning Policy**, and **Remote Learning Plan.**

Purpose

The primary purpose of this document is to establish a set of rules and regulations to enable all users of the Internet, PC's, and mobile devices to do so for the benefit of the school.

Additionally, this document aims to safeguard authorised users. Specifically, to:

- Minimise (and where possible eliminate) the school's legal liability for the acts of authorised users using the Internet, PC's, and mobile devices.
- Minimise (and where possible eliminate) the threat of damage to the school property and or reputation by acts of authorised users using the Internet, PC's, and mobile devices.

- Educate authorised users on their duties and obligations to the school and each other when using the Internet, PC's and mobile devices and the consequences of breaching them
- Protect authorised users if the **Online Safety & Acceptable Usage Policy** is breached by accident.

School Responsibilities

The implementation of this policy should be carried out so that:

- Every authorised user with Internet access is aware of the policy and understand its contents.
- Its regulations are enforced throughout the school.
- Breaches can be reported in a safe and confidential manner.

Staff are reminded/updated about online safety regularly and new staff receive information on the school's **Online Safety & Acceptable Usage Policy** as part of their induction. Teachers must sign the **'Authorised Users Agreement'** before using the Internet, PC's, or any mobile devices in school.

Security and Data Protection

The school and all staff members comply with the Data Protection Act 2018 (DPA) and General Data Protection Regulations 2018 (UK GDPR). Personal data will be recorded, processed, transferred, and made available according to UK GDPR. Password security is essential for staff, particularly as they can access and use pupil data. Staff have secure passwords which are not shared with anyone. Any confidential or sensitive information such as pupil reports or SEND information must be kept secure and staff will use an encrypted and password protected email to ensure any transfer of documentation is secure. All users (Staff, trainee teachers, agency staff and governors) read and sign an **'Authorised Users Agreement' (see Appendix A(ii))** to demonstrate that they have understood the school's **Online Safety and Acceptable Usage Policy.**

Warning against Deliberate Misuse of the Internet

The Internet is a valuable resource. It also presents significant dangers to the school from staff who may choose to abuse it. Whilst each case will be judged on its own merits any member of staff who commits a breach of school policy as a result of unauthorised use of the Internet (including email) PC's and mobile devices will be subject to disciplinary procedures in line with school policies.

Protection of Staff acting in good faith

It is fully recognised that a member of staff may accidentally breach the **Online Safety and Acceptable Usage Policy** whilst acting in good faith and in the course of their duties as a member of staff of the school. If a member of staff suspects this to be the case, they must notify the Computing Subject Leader, Deputy Headteacher or Headteacher immediately so that action can be taken to prevent or minimise damage and incidents can be logged.

Authorised uses of the Internet using school property whilst on school premises

The school permits staff to use the Internet whilst in school in connection with school related matters only. This may include.

- The delivery of Computing/subject specific lessons.
- Searching for lesson resources.
- Checking and responding to school emails using only school email logins.
- Other school related searches.

Please note that users may be asked to justify accessing any site and web content accessed using a school device and is regularly monitored by the Deputy Headteacher in conjunction with the Local Authority. A list of all websites accessed and details of staff who have accessed a site not obvious for school use, will be passed on immediately to the Headteacher and investigated.

Unauthorised uses of the Internet

Whilst an act that does not fit the above categories will be considered an unauthorised use of the Internet, all user's attention is drawn to the following:

Strictly Prohibited Acts

- The copying of software files from the Internet must only be done within the parameters set in this policy.
- No executable files should be copied from the Internet. Software downloads must only be carried by an authorised admin user who can ensure that it is not faulty, it is not infected with a virus and that all copyright requirements are met. If there is any doubt the North Tyneside IT Manager should be contacted via the Headteacher.
- Do not access any sites or download or print any files displaying material that the users know contravene the school's Equality & Diversity Policy. If such a site is accessed inadvertently inform the Computing Subject Leader /Headteacher immediately.
- Do not access any site that involves any form of gambling or betting.
- Do not access any sites which provide a discussion or 'chat' forum which does not fit the authorised uses above e.g. Early Years Forum is acceptable but not social media sites unconnected with a professional account.
- Do not access personal email (Hotmail, etc) during school hours.
- Do not respond to surveys on the Internet on behalf of the school without consulting the Headteacher.
- Do not open a subscription account on the Internet on behalf of the school without express permission of the Headteacher.
- Do not use email for communication other than for purposes set out in Authorised Uses of the Internet.
- Do not leave school iPads in a state where it would be possible for someone other than the normal user, or authorised user, to access the Internet. Staff are responsible for logging off or locking an iPad when it is not in use. iPad trolleys must be locked and returned to the IT Suite at the end of the school day or prior to the member of staff departing.
- Do not leave your PC, school iPad or any other mobile devices unattended without locking it or ensuring it is password protected.

It is the responsibility of all users to report any unauthorised acts as soon as it comes to their attention to the Headteacher who in turn should investigate the data breach in consultation with North Tyneside IT Manager and in line with UK GDPR.

Electronic media access on school iPads whilst not on school premises

School iPads are for the *sole* use of the person to whom they were issued and should only be used in preparation for lessons and school related work.
Additionally, users are requested to follow the principles of good practice set out below.

Internet

- Do not reveal your own (or any other person's) personal details e.g., home address, telephone number over the Internet.

School email

- Email should only be used in the course of your work as a school employee and only using the authorised logins provided by the school.
- Email is not a person-to-person communication and should always be written using appropriate language.
- Never use email to send or forward chain letters or any material which may contravene school policies (e.g., jokes, pictures of a racist or sexist nature)
- Only copy messages (i.e., cc or bcc) to people where it is of direct relevance.
- Check your mailboxes regularly, at least once a day, when in school.
- Ensure that messages arriving in your mailbox are forwarded to another person if you are on leave for an extended period
- Do not use your school email for personal matters
- Emails may be monitored by North Tyneside IT Services.

Reviewing this Policy

This policy will be reviewed every year, or sooner, as the use of the Internet and use of electronic media in school develops. If you have any comments about this policy, please pass them on to the Computing Subject Leader, Deputy Headteacher or Headteacher.

Appendix A(ii)

Authorised Users Agreement

This is to be signed individually by all authorised users (staff, governors, trainee teachers and agency staff) prior to their use of electronic media.

I have read the school's **Online Safety and Acceptable Usage Policy, Staff Information Systems Code of Conduct** and **Social Networking Policy** and accept that it forms part of my conditions of employment.

Employee's Name

_____

Employee's Signature

_____ Date_____

Headteacher's Name

_____

Headteacher's Signature

_____ Date_____

Appendix A(iii)

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's policies on Social Networking, Safeguarding & Child Protection and Online Safety & Acceptable Usage for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may NOT be used for private purposes whilst on school premises, e.g., accessing personal email accounts and personal internet use.
- I will use my school email account for sending and receiving emails for work related purposes only and no other email accounts on school computers.
- I will only use the internet for work related purposes whilst at school or whilst logged into a school account using a school PC or iPad.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will NOT disclose any passwords or security information to anyone other than an appropriate system manager.
- I will NOT download or install any software or hardware without prior permission.
- I will ensure that pupil's personal data is kept secure and is used professionally and appropriately in school. I will NOT take pupil's personal data off the school premises.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school Computing Subject Leader and Designated Safeguarding Lead or Deputy Designated Safeguarding Leads.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- Network access must be made only via the user's authorised account and password, which must NOT be given to any other person.
- I will only use social networking sites for professional purposes. e.g., Using a professional X(formerly Twitter) account for education purposes is permitted.
- Use for personal financial gain, gambling, political purposes, or advertising is NOT permitted.
- The school may exercise its right to monitor and log the use of the school's information systems, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery, or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Print Name: …… Date:……...

Appendix B(i)

Dear Parent/Guardian,

In order to showcase the learning that takes place in and out of Redesdale Primary School, staff regularly take photographs and videos of the children at our school. These recordings may be used in our school for displays, in the children's books as evidence of their work and on our school website or X(formerly Twitter) account to share with the school community. They will also be securely stored on our secure servers and cloud-based storage (Microsoft 365).

Sometimes our school may be visited by the media who will take photographs of an event. Pupils will often appear in these images which may appear in local or national newspapers.

In order to comply with the UK General Data Protection Regulation 2018 (UK GDPR) the school and Local Authority needs your permission before we photograph or make a recording of your child. I would be grateful if you would complete this form, sign, date it and return it to school as soon as possible. If you have any questions about this matter, please contact the school office to discuss it further.

Yours sincerely,

M. J. Shackleton

Deputy Headteacher & IT Lead

Appendix B(ii)

Media Consent Form

Conditions of Use

This form will be used to celebrate your children's learning and achievements and assist with the wider promotion of the school.

We will not:

- use personal details or full names of your children in photographic images; on video; on our website or on X(formerly Twitter)
- include personal Online mail or postal addresses, or telephone and fax numbers in photographic images; on video; on our website; or on X(formerly Twitter)

Please note that images of children used in the scenarios below are NEVER released along with personal information about your child (without your explicit permission for this to be credited to them, and only ever in exceptional circumstances to celebrate specific achievements).

Name of child: _____

In order to celebrate learning and achievement, I agree that:

Please circle your answers below:

The school may use photographs / videos of my child on the school website	Yes / No
The Local Authority may photograph/video my child and use the images to celebrate learning. ***For example, at sporting events / festivals / during learning activities***	Yes / No
My child may appear in the media (images / video) in print (newspapers, flyers, promotional material) and online (including websites and social media) in connection with school activities. ***For example, a local museum may wish to use photographs of an event in their magazine, on their website or on their Social Media Channels.***	Yes / No
The school may record and store photographs and video of my child on its own secure servers, and cloud-based storage. ***For example, curriculum evidence.***	Yes / No
The school may choose to use appropriate educational provider's platforms to support learning in school and upload photographs and video of my child to their secure servers and cloud-based storage. ***For example, Seesaw; Target Tracker.***	
The school / individual staff members may post photographs and videos of my child on the school X(formerly Twitter) account and their own professional X(formerly Twitter) accounts. ***For example, to showcase the learning taking place in and out of the classroom.***	Yes / No
The school may use photographs of my child for various printed publications used to promote the school. ***For example, newsletters, pamphlets, school prospectus, special event flyers etc.***	Yes / No
I agree that my child may participate in school-based collaborative projects, including online communication with other schools and educational providers. ***For example, Microsoft Teams / Zoom / Google Meet conversations with authors / online learning visits etc.***	Yes / No

I confirm that I have read and understood the **conditions of use** on this form.

Signature of Parent/Guardian: _____

Name of Parent/Guardian (capitals): _____

Date: _____

Appendix C: Online Safety Rules Letter

REDESDALE PRIMARY SCHOOL
Wiltshire Drive, Wallsend, Tyne & Wear NE28 8TS
Tel: (0191) 814 9435 Fax: (0191) 262 3093
Email: office@redesdaleprimary.org.uk
Website: www.redesdale.co.uk Twitter: @RedesdalePrim

Headteacher: Mrs. T. V. Flannaghan B.Ed. (Hons), NPQH

Dear Parent/ Carer

By teaching Computing as part of the National curriculum, we aim to ensure that pupils leave Redesdale Primary School as digitally literate individuals – able to use, and express themselves and develop their ideas through, information and communication technology (ICT) – at a level suitable for the future workplace and as active participants in a digital world.

A hugely important part of this learning is understanding how to use technology safely, respectfully, and responsibly, keeping personal information private; recognising acceptable / unacceptable behaviour and identifying where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Please read and discuss these Online Safety Rules with your child and then keep the Online Safety Rules at home for your reference. If you have any concerns or would like some explanation, please contact your class teacher. Please take care to ensure that appropriate Online Safety systems are in place at home to protect and support your child/ren.

Please complete the section below and return the form to school. This will be kept on record for the duration of your child/ren's time at Redesdale Primary School.

Mrs T V Flannaghan

T.V. Flannaghan

Headteacher

Parent/ carer signature

We have discussed this document with …..... (child's name) and we agree to follow the **Pupil Online Safety Agreement and Rules** and to support the safe use of ICT at Redesdale Primary School. I understand that any misuse of these Online Safety Agreements and Rules may result in my child/ren having their ICT access removed.

Parent/ Carer Signature ……

Class …… Date ……

Appendix D(i): Pupil Online Safety & Acceptable Usage

The school has developed a set of rules to help keep pupils safe whilst using digital technology e.g., Internet, email, mobile phones, smart watches or devices, portable gaming devices and tablets. Pupils will be reminded of their responsibilities whilst using digital technology in school. These rules will be kept under constant review and amended as required. Pupils **MUST** obtain the permission of their parent/guardian/carer before they can be allowed to use the internet/email system in school. The Parental Permission section **MUST** be signed and returned to the school.

The following rules apply to ALL pupils:

- I will be responsible for my behaviour when using technology because I know these rules are to keep me safe.
- I will use school equipment and resources responsibly and with respect when directed by my teacher or member of staff. I will take full responsibility for damage caused to school equipment if used inappropriately.
- I will only use my own login and password that has been given to me by my teacher when logging onto school computers or online resource sites (For example, Times Table RockStars) and will keep it secret.
- I will only use the internet in school for schoolwork and follow my teacher's or member of staff's instructions.
- I will turn off my monitor (screen) and tell my teacher or member of staff IMMEDIATELY if I see anything on the internet that makes me feel unhappy or uncomfortable.
- I will turn off my monitor and tell my teacher or member of staff IMMEDIATELY if I receive any digital communication that I don't like.
- I will only send digital communications that are polite and sensible.
- I will NEVER give out my own or others personal details e.g., name, address, phone number, etc.
- I will support the school approach to online safety and NOT deliberately download or upload any images, videos, sounds or text that could upset any member of the school community.
- I know that the school may check my files and monitor the internet sites I visit. The school may contact my parent/guardian/carer if the school is concerned about my online safety.
- I will NOT bring data storage devices (USB sticks, memory cards, etc) into school and use them on any school devices.
- I will NOT bring my mobile phone in to school without my parent's knowledge and only if my parent/guardian/carer has provided school with their permission.
- I will turn off my mobile phone, put it in to the class mobile phone box to be handed into the office and leave it there for the duration of the school day if I have parental permission to have it in school.
- If I am accessing Microsoft Teams outside of school for home learning or remote learning, I will ensure my behaviour is in line with school expectations (PROUD)
- When using Microsoft Teams for remote learning, I will follow the instructions given to me by my teacher and will ensure my camera and microphone are turned off. If I am asked to contribute to the learning discussion, I will turn on my microphone when instructed. I will never use ICT in an offensive way that may hurt others.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement when I am outside of school and where they involve my membership of the school community. I understand that if I deliberately break these rules, I may be stopped from using equipment and resources.

Appendix D(ii)

Online Safety Agreement for Foundation Stage and KS1 pupils

- I understand that my school wants me to enjoy using the Internet and a range of digital technologies to help my learning. I know I must use them in a responsible way.
- I will only use the Internet to search for information when an adult is with me.
- I know that I need to think before I click buttons that I do not know about and ask an adult if I am unsure.
- If I see something that I do not like I will turn off the screen and tell an adult.
- I will not do anything that will upset other children when I use the school's technology equipment.
- I will not bring my mobile phone or any other mobile devices to school.

Please tick and sign below if you agree.

Pupil:

☐ I know any rules we have are here to help me keep safe and I agree to follow them.

☐ If I break these rules, I may be stopped from using the computers or internet in school.

Name: _____ Date:_____

Parent:

I have read and understood the school online safety rules and give permission for my child to access the Internet and other digital technologies for educational purposes. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of material accessed through the internet but know that strict filtering systems managed by North Tyneside are in place to prevent this happening.

☐ I have read the rules and discussed them with my child.

Name: _____ Date:_____

Appendix D(iii)

Online Safety Agreement for KS2 pupils

- I understand that my school wants me to enjoy using the internet and technologies to support my learning. I know I must use them in a responsible way.
- I understand that my teachers will help me know what is acceptable and unacceptable when using computers, the internet, mobile phones, email, online communities and mobile devices and I will listen carefully to the advice I receive.
- I will not bring mobile phones/mobile devices into school unless there are special circumstances.
- I will only use the internet under the direction of a responsible adult.
- I know that when I use the internet, I must use search engines safely and choose appropriate content from the search results I am presented with.
- I will never try to access personal email or chat rooms from the school network.
- If I see something that I do not like I will turn off the monitor and tell an adult.
- I will keep my passwords a secret and not share them with others.
- I will only access my own work on the school network.
- I know that all my communications with other people using ICT should be polite and friendly and I will not deliberately send anything unfriendly or nasty.
- I will not give anybody's personal details including my own, such as name, address or phone number to anyone and I will **not** agree to meet them.
- I understand that when I am in school, I must only use the Microsoft Teams chat function for schoolwork related reasons and know that school can view any content that I add to this chat.
- I understand that if I am using Microsoft Teams outside of school to access remote learning, I must behave in the same way as I would in school, following the PROUD rules and any instructions given to me by a teacher or member of school staff.
- I know that the school can check my computer files and the internet sites I visit and that if there are any concerns about my safety, staff will contact my parent or carer.

Please tick and sign below if you agree.

Pupil:

☐ I know any rules we have are here to help me keep safe and I agree to follow them.

☐ If I break these rules, I may be stopped from using the computers or internet in school.

Name: _____ Date:_____

Parent:

I have read and understood the school Online safety rules and give permission for my son/daughter to access the internet for educational purposes. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of material accessed through the internet.

☐ I have read the rules and discussed them with my child.

Name: _____ Date:_____

Appendix E **Mobile Phone ONLINE Safety Agreement & Rules**

REDESDALE PRIMARY SCHOOL
Wiltshire Drive, Wallsend, Tyne & Wear NE28 8TS
Tel: (0191) 814 9435 Fax: (0191) 262 3093
Email: office@redesdaleprimary.org.uk
Website: www.redesdale.co.uk Twitter: @RedesdalePrim

Headteacher: Mrs. T. V. Flannaghan B.Ed. (Hons), NPQH

Dear Parent/ Carer,

Governors and staff acknowledge that as children get older, they should have increasing responsibility. Parents may choose to allow older children to have mobile phones. On occasions children are permitted to have mobile phones so that they can contact parents if they are walking home from school unaccompanied. This is considered acceptable for children in Years 5 and 6.

However, children should not have mobile phones during the school day at school under any circumstances. Therefore, children in Years 5 and 6, who are given permission by parents to carry mobile phones to school with them, must hand them in to their Class Teacher so that they can be sent to the school office for safe keeping.

If children are found to be using phones in an inappropriate manner, they will be confiscated and returned to parents. That child may not be permitted to bring a phone into school again. Please complete the slip below and return it to school if you have a child in Year 5 or 6 and would like them to have a mobile phone for their journey to and from school.

Thank you for your co-operation in this matter

Mrs T V Flannaghan

T.V. Flannaghan

Headteacher

Y5 / Y6 ONLY – Mobile Phones e-Safety Agreement and Rules

- Pupils in Years 5 and 6 are allowed to bring personal mobile phones into school but they must be handed in to the School Office during morning registration
- The devices must be switched off as soon as the pupil comes onto the school premises
- The school is not responsible for the loss, damage or theft of any personal mobile device
- Users bringing personal mobile phones into school must ensure there is no inappropriate or illegal content on the device.

Parent/ carer signature

I give permission for ……..... (child's name) to bring a mobile phone for the journey to and from school. I understand that it will be held in the School Office until home time. I accept that if my child uses the phone inappropriately it will be confiscated and returned to me, the parent. I understand that my child / children may not be permitted to bring their mobile phone into school should they choose NOT to follow our **Mobile Phone Online Safety Agreement and Rules**.

Parent/ Carer Signature: …… Date: ……