Rowlands Gill Primary School

ICT (Computing) and

Online Safety Policy

Date Written: July 2020

Ratified by Governors: November 2020

Re-adopted by Governors: February 2024

Next Review Date: February 2025

Policy review dates:

Review Date	Changes made	By whom	Date Shared
September 2022	Removed SBM, slight updates with new technology	Lindsey Clarke	October 2022
March 2023	Updated online safety at home	LC	20.3.23
January 2024	New AUP statements for all parties in appendix	LC	5.2.24

Intent

It is our intention to enable children to find, explore, analyse, exchange and present information using technology. We also focus on developing the skills necessary for children to be able to use information in a discriminating and effective way. We want children to know more, remember more and understand more in computing so that they leave primary school computer literate. Computing skills are a major factor in enabling children to be confident, creative and independent learners and it is our intention that children have every opportunity available to allow them to achieve this.

We have built a computing curriculum that develops pupil's learning and results in the acquisition of knowledge of the world around them; that ensures all pupils can understand and apply the fundamental principles and concepts of computer science. We want our computing curriculum to prepare pupils to live safely in an increasingly digital society where pupils can evaluate and apply information technology analytically, including new or unfamiliar technologies, to solve problems.

Implementation

- A clear and effective, scheme of work that provides coverage using the best sources in line with the National Curriculum. Teaching and learning should facilitate progression across all key stages within the strands of digital literacy, information technology and computer science.
- Access to resources which aid in the acquisition of skills and knowledge.
- Children will have access to the hardware (computers, tablets, programmable equipment) and software that they need to develop knowledge and skills of digital systems and their applications.
- Children will have the opportunity to explore and respond to key issues such as digital communication, cyberbullying, online safety, security, plagiarism and social media.
- Wider curriculum links and opportunities for the safe use of digital systems are considered in wider curriculum planning.
- The importance of online safety is taught in lessons and assemblies and reminders are provided through displays within the learning environment.
- SLT and parents are informed when issues relating to online safety arise and further information/support is provided if required.

Impact

- Children will be confident users of technology, able to use it to accomplish a wide variety of goals, both at home and in school.
- Children will have a secure and comprehensive knowledge of the implications of technology and digital systems. This is important in a society where technologies and trends are rapidly evolving.
- Children will be responsible and respectful digital citizens who know how to behave online.

Online Safety and Acceptable Use

Online safety encompasses internet technologies and electronic communications such as mobile phones, iPads and wireless technology. Most young people are enthusiastic Internet users - particularly of interactive services like email, chat and instant messaging. However, like many exciting activities, there are risky situations to deal with and hazards to avoid. Robust policies and procedures, clear roles and responsibilities, a comprehensive online safety education programme for pupils, staff and parents and an effective range of technological tools to support online use are essential to providing a safe Computing learning environment.

Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using technology, media and information resources, is one that the school shares with parents and carers. At Rowlands Gill Primary School, we feel that the most successful approach lies in a combination of site filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Context

Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant messaging / video messaging (e.g. Skype) using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Smart phones with camera and video functionality
- Smart phones, tablets and Ipads with e-mail, web functionality and cut down 'Office' applications.

Computers are now part of everyday life, and the following link shows the government strategy for education technology. https://www.gov.uk/government/news/edtech-strategy-marks-new-era-for-schools

For most of us, technology is essential to our lives, at home and at work. Being 'digitally literate' is a skill which children must be taught if they are to be ready for the workplace and able to participate effectively in this digital world. The national curriculum for Computing has been developed to equip young people in England with the foundational skills, knowledge and understanding of computing they will need for the rest of their lives.

Through the programme of study for Computing, they will learn how computers and computer systems work; they will design and build programs; develop their ideas using technology and create a range of content. Children who can think computationally are better able to conceptualise, understand and use computer-based technology, and so are better prepared for today's world and the future.

Across the curriculum, children learn to:

- Find and select information from digital and online sources, making judgments about accuracy and reliability.
- Create, manipulate and process information using technology to capture and organise data, in order to investigate patterns and trends; explore options using models and simulations; and combine still and moving images, sounds and text to create multimedia products.
- Collaborate, communicate and share information using connectivity to work with, and present to, people and audiences within and beyond the school.
- Refine and improve their work, making full use of the nature and pliability of digital information to explore options and improve outcomes.

Online Safety at Home

Our school plays a critical role in promoting online safety and digital citizenship, not just within the school environment, but also in pupils' homes. Educational resources are provided, via a dedicated page on our school website, to parents and guardians. These include tips on how to monitor their child's online activity, how to set age-appropriate boundaries, and how to teach their children about safe online behaviour. Workshops and training sessions are organised each year for parents to help them navigate online safety issues. Furthermore,

our school collaborates with official organisations to offer expert guidance and support on topics such as cyberbullying, online predators, and social media influence. By taking a proactive approach to online safety, our school helps to empower families to take ownership of their digital lives and create a safer and more positive online community.

When children complete homework online this is also provided through safe, secure websites which have been approved by school staff. If children are set research tasks, parents will be alerted that this activity should be supervised in case of inappropriate content being able to get through home filtering systems.

If children experience issues with online safety at home, school will do all we can to offer guidance or support, acknowledging that there will be obvious limitations in what we can do to ensure filtering etc is appropriate in the home.

Recording Children's Work in Computing

In some Computing lessons, the program Seesaw or Google Education will be used to record children's computing learning journey. Children are taught how to document their learning. They are able to use the tools in Seesaw to explain what they have produced in lessons. Every child will have their own portfolio and these will be archived every year.

Policies and Procedures

- The school's Online Safety policy will operate in conjunction with other policies including: Behaviour, Anti-Bullying, Safeguarding and Data Protection.
- It has been approved by governors.
- The Computing and Online Safety Policy and its implementation will be reviewed annually and where necessary in cases of reported misconduct or risks.
- All Rowlands Gill, staff, parents and pupils are asked to sign an Acceptable Use Policy (AUP) detailing the ways staff, parents, pupils and all network users should use our ICT facilities and reflects the need to raise awareness of the online safety issues associated with electronic communications as a whole.
- Online safety will form a key part of the Computing/PSHE curriculum. Children will be made aware of the dangers and risks of using the internet and mobile technologies throughout the school year. This will include learning about issues during Anti-Bullying/Internet Safety Week and will form an integral part of Computing lessons.

All staff (including teachers, admin staff, supply staff and classroom assistants) and any other adults involved in supervising children accessing the Internet, will be provided with the Online Safety and Acceptable Use Policy, and will have its importance explained to them. Parents' attention will be drawn to the policy by letter in the first instance and, thereafter, in our school admissions pack and on the school's website. The policy is available for parents and others to read on the school website and on demand.

We have a major responsibility to educate our pupils, 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. Yet at the same time, we recognise that the use of these new technologies can put young people at risk within and outside the school environment.

The most serious risk to children using the internet involves the possibility of someone being hurt, exploited or abused as a result of personal information being disclosed online. Pictures, names, addresses, ages or information about a child's likes or dislikes can be used to trace, contact and meet a pupil with the intention of causing harm.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content

- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school. For example, school and personal data being entered on web/social networking sites, fraudulent email traps and cyberbullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision to manage the risk and deal with any threat to safety.

The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access.

Internet Access

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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.
- The school's internet access is designed expressly for pupil use and uses the **Omnicom Service** and filtering system.
- Pupils are taught which internet use is acceptable and which is not and are given clear objectives for internet use. Pupils will not use the internet without having permission and **MUST be supervised at all times by a member of staff.**
- All school devices are monitored by 'Securus' software which captures any searches made for inappropriate materials or any incidents of inappropriate content being viewed. The captures are sent to the Headteacher who will investigate and take action as appropriate.

All staff are aware that a filtering and monitoring system can reduce but cannot eliminate the risk of exposure to inappropriate material on the internet. This is why no child must be allowed to access the internet without adult supervision.

Staff laptops and devices MUST be locked when not in use. There is encryption software on staff laptops, but they should not be left unattended at school or at home when logged in.

Our children use individual pupil logins to access our school network as soon as it is appropriate for them to do so (according to their age). For some children, year group logins are used as a first step.

All members of staff have individual, password protected logins to the school network. Supply teachers, visitors and community users have a generic login and password which is changed regularly.

The school's network can either be accessed using a wired or wireless connection. The wireless network is encrypted to the standards advised by **Omnicom** and the wireless key is kept securely by the school office and Headteacher.

Certain sites are blocked by Omnicom and it is at the Headteacher's discretion to unblock them via Omnicom.

School staff, visitors and pupils are NOT permitted to connect personal devices to the school's wireless network. (Exception to this rule will be at the discretion of the Headteacher.)

- Pupils will not use social networking sites (these are blocked) in school and will be educated about their safe usage in their own time. Parents will also be educated in these areas during online safety workshops.
- Pupils will be advised to never give out personal details of any kind which may identify them, their friends or their location. **(Reference to YAPPY in KS2 will be made – Your name, Address, Password, Phone number or Your plans).**
- Pupils are forbidden from downloading games or other programmes from the internet.
- Downloading programs from the internet will be carried out by the IT technician or Computing subject leader.
- Public chatrooms and instant messaging are **not allowed** and are blocked using the school internet filter.
- Pupils will be educated in 'Information Literacy' and taught how to evaluate the internet content that they have located. Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law. Pupils will be taught to reference materials they have found from other sources so as not to infringe copyright or the intellectual property of others.
- Pupils will be taught how to report unpleasant internet content.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by complying with the rules for acceptable computer use, which have been designed to help protect them from exposure to internet sites carrying offensive material. A most important element of our acceptable computer use agreement for pupils is that they will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable. If there is an incident in which a pupil is exposed to offensive or upsetting material the school will respond to the situation quickly and on a number of levels.

Procedures for Reporting Inappropriate Content

All staff who believe that an inappropriate item has breached the filter should report it to the Computing leader or Omnicom immediately. The Headteacher or Admin Officer can access a log of all inappropriate content via Omnicom if necessary. The first report may well be a Securus capture received by the Headteacher.

Responding to Incidents

Minor Incidents of Misuse - Pupils

This might include:

- Copying information into projects and failing to acknowledge the source (plagiarism and copyright infringement)
- Downloading materials or images not relevant to their studies, in direct breach of the school's acceptable use policy
- Misconduct associated with logins, such as using someone else's password.

In most minor of cases the pupil should be issued with a warning by their class teacher, and the incident reported to the Computing Leader, so that documentation is kept. An incident report should be completed by the class teacher on CPOMs. If the behaviour is repeated, or the misconduct escalates, it can then be responded to more seriously because there is evidence of previous events. If pupils abuse the privileges of access to the internet or use of e-mail facilities, then sanctions consistent with our School Behaviour Policy will be applied. This may involve informing the parents/carers. Access to computers and/or the internet may be denied for a fixed period.

Responding to Inappropriate or Illegal Incidents

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology. Responding to an online safety incident in school is no different to responding to other incidents in school.

If an online safety incident occurs, the school will follow its usual procedures for dealing with other incidents including internal sanctions and involvement of parents (for IT, this may include the deactivation of accounts or restricted access to systems as per the school's AUPs).

It is very important that appropriate procedures are in place and adhered to for responding to such instances. Our Computing Leader acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with our Safeguarding Policy by the Designated Safeguarding Lead (DSL). All the teaching staff will be made aware of the incident at a Staff Meeting if appropriate. Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed.
If a concern is raised, refer immediately to a DSL or the Chair of Governors.

It is their responsibility to take the following steps:

Step 1
Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator.

Step 2
Establish the kind of activity involved and whether it is inappropriate or illegal. If in doubt, consult the helpline offered by Clenell Safeguarding Services.

Examples of inappropriate activities:
While not illegal, there will be some material that is just not appropriate within the school environment, and, in the case of staff, not in keeping with the professional standards or code of ethics of those who work with children and young people. Some examples are;

- *Deliberately accessing, printing, showing or transmitting inappropriate (or age-restricted) material within the school's network. Even if such material was not deliberately accessed by the pupil, but not reported to a teacher, and was subsequently shown to other pupils, this should also merit a disciplinary response.*

Examples of illegal activities:
In the school context, very serious incidents tend to involve illegal materials (particularly the viewing, possession, making and distribution of indecent images of children) or serious stalking or harassment facilitated by communication technologies. Such criminal offences may be committed by staff and pupils alike. Some examples are:

- *Indecent images of children are defined under Section 7 of the Protection of Children Act 1978 (as amended by Section 84 of the Criminal Justice and Public Order Act 1994). References to indecent photographs under the Act include data stored on a computer disk or by other electronic means that is capable of conversion into a photograph.*
- *The Protection from Harassment Act 1997 is intended to prevent 'stalking' and other similar unsocial conduct. It states that a person must not pursue a course of conduct which amounts to harassment of another, and which he/she knows, or ought to know, amounts to harassment of the other. Although the term is deliberately not defined in the Act, words such as 'alarm',' distress' or 'torment' fit the term most accurately, and some adverse impact on the victim is required. To constitute a 'course of conduct', harassment must take place on a minimum of two occasions.*

Step 3
Ensure that the incident is documented on CPOMs or using the standard safeguarding incident form which is available from the HT/DHT.

Depending on the judgements made at steps 1 and 2 the following actions should be taken:

Staff instigator – follow the standard procedures for Managing Allegations Against a Member of Staff. If unsure seek advice from the Local Authority Designated Officer.

Staff victim – Seek advice from Clennell Safeguarding Services - if it is a child protection issue.

Incidents that involve inappropriate but legal material will be dealt with by the school via the usual disciplinary system; unless a criminal offence has been committed, it will not normally necessary to involve the police. Disciplinary action may range from a warning to dismissal of a staff member or suspension of a pupil. As in all disciplinary instances of this seriousness, the school will follow disciplinary protocols, ensuring that proper documentation and recording of information occurs, and that appropriate counselling and support are given, and ensuring that parents and carers of the pupil involved are kept fully informed of the matter.

Discovery of indecent material within the school's network is a very serious situation and must always be reported to the police. The following procedures MUST be adhered to:

- *Evidence must be immediately secured.*
- *The equipment concerned must be isolated.*
- *No attempt should be made to investigate the incident – the matter must be referred to the Police to review suspect equipment. Staff should never attempt to access a website which they believe to be illegal – to do so would technically break the law and make them liable to prosecution. If there is any doubt about the subject matter, it is enough to view the Internet history. Any attempt to follow the Internet hyperlinks to the sites themselves will invalidate evidence by updating the time stamps of images received. Material must not be downloaded, printed or sent by email because doing so is an offence in itself.*
- *No member of staff is allowed access to the equipment once this procedure has been implemented.*
- *The school will seek legal advice as soon as possible, particularly with regard to disciplinary actions that are acceptable while the police carry out their investigations.*

Review Following a Serious Incident
In the event of a very serious incident occurring within school, a review of all online safety policies and procedures will be conducted as soon as possible. The Headteacher has ultimate responsibility for the review process but may delegate this to the school's Computing subject leader.

The three key components of a safe ICT learning environment (the infrastructure of whole-school awareness, designated responsibilities, policies and procedures; the effective range of technological tools; and a comprehensive internet safety education programme) will also be reviewed, ensuring that:

- Comprehensive debriefing occurs after the incident to maximise what can be learnt.
- The ICT technician has the professional skills to carry out regular safety checks and knows the correct protocols to follow if illegal material is suspected or encountered.
- All school staff understand the circumstances under which a forensic audit of computers should be carried out, and by whom, and the appropriate strategies to adopt to ensure that evidence is secured and preserved.
- The school's Computing subject team contains staff with all the relevant expertise, and that the appropriate time and authority is allocated to the team to allow them to carry out their duties effectively.

Email

- When available, pupils may only use approved school e-mail accounts (provided by the school). Pupils are not permitted to use their own personal email accounts on school equipment.
- Before using school e-mail accounts, children will agree to guidelines on how to use email and how to stay safe.
- Pupils must immediately tell a teacher if they receive an offensive e-mail and are asked to keep the email in order to show the adult.
- In e-mail communications, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.
- Incoming e-mails should be treated as suspicious, and attachments not opened unless the author is known.
- Emails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- **Staff should never use personal email addresses to communicate with pupils or parents. An official school email address will be provided by the Admin Officer.**

Photographs/ videos and published content and the school website

- Parental permission for our use of images of their child will be sought on entry to school (via the admission pack).
- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website. **Pupils' full names will not be used anywhere on the Website or Blog, particularly in association with photographs.**
- Work can only be published with the permission of the pupil and parents.
- Pupil image files should be securely stored on the school network or Microsoft 365 Cloud Based System.

STAFF WILL BE INFORMED OF ANY CHILDREN WHOSE PHOTOGRAPHS SHOULD NOT BE TAKEN, VIA ARBOR.

Parents Taking Photographs / Videos

Under the Data Protection Act (1998), parents are entitled to take photographs of ***their own*** children on the provision that the images are for ***their own*** use, e.g. at a school production. Including other children or other purpose could constitute a potential breach of Data Protection legislation.

For this reason, at any school event e.g. Christmas Play, parents are informed that they should only take photographs of their own children at the end of the production and that they need permission to include any other children / adults. Where possible, school will take individual photos of children in their costumes and share individually with the parents.

Parents are always reminded that publishing images which include children other than their own or other adults on Social Network sites is not acceptable, unless specific permission has been obtained from the subjects.

Portable Devices

- **Children will not use mobile phones during school time and on school property. For children who walk home alone, phones must be handed in to the class teacher at the beginning of the day. The appropriate consent form for bringing a mobile into school must have been completed by the parent or carer before a child brings their phone in. This is available from the school office. The sending of abusive or inappropriate text messages is forbidden and children are educated what to do in case this happens.**

STAFF MUST NOT USE THEIR MOBILE PHONES IN THE CLASSROOM WHEN THE CHILDREN ARE PRESENT. MOBILE PHONES SHOULD BE KEPT ON SILENT IN A PERSONAL BAG OR LOCKED DRAWER. STAFF MAY USE THEIR MOBILE PHONES DURING BREAKTIMES AND LUNCHTIME. (IF THERE ARE NO CHILDREN PRESENT)

- Staff should be aware that technologies such as Ultra Portable Laptops, Nintendo DS devices, iPads and tablets and mobile phones may access the internet by bypassing filtering systems and present a new route to undesirable material and communications. Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access which may not include filtering. **These may not be used in school.**

- Staff should **NOT** use their personal mobile phones to contact pupils or capture photographs of children. Neither should they use personal cameras to take photographs. Alternative equipment will be provided by the school.

Occasionally, there may be an extreme situation where a member of staff needs to use their own equipment. This should only ever occur having first sought the permission of the Headteacher.

Where this has been agreed, all staff must transfer photos/video taken on personal devices onto the school secure network within a maximum of 24 hours. Materials must then be immediately deleted from the device.

Social Networks

Social Network sites allow users to be part of a virtual community. Current popular examples of these sites are Facebook, Twitter, Snapchat, Instagram, Tik Tok, Club Penguin and Moshi Monsters (for children). These sites provide users with simple tools to create a profile or page including basic information about themselves, photographs, and possibly a blog or comments. As a user on a Social Network site, you may have access to

view other users' content, send messages and leave unmediated comments. Many Social Network sites are blocked by default through filtering systems used in school, but these settings can be changed at the discretion of the headteacher.

Although use of Social Networks tends towards a personal basis outside of the school environment, their use as a tool for communicating with parents is becoming more commonplace in primary schools. Guidance for personal use of social networking, and personal publishing sites is included as part of staff induction, discussed regularly and outlined in the staff Acceptable Use Policy – along with sanctions for inappropriate use.

If a school Social Network page is to be created, consideration must be given to the purpose and audience, ensuring that the privacy settings and interaction are appropriate.

Remember; whatever methods of communication are used; individuals should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and potentially remains there forever.

All staff need to be made aware of the following points:

- The content on Social Network sites may be unmediated and inappropriate for certain audiences.

- If a Social Network site is used personally, details must not be shared with children and privacy settings be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.

- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.

The content posted online should not:

- bring the school into disrepute
- lead to valid parental complaints
- be deemed as derogatory towards the school and/or its employees
- be deemed as derogatory towards pupils and/or parents and carers
- bring into question their appropriateness to work with children and young people.

Adults must not communicate with children using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted. Online communications with parents, past pupils or siblings of pupils, especially if under the age of 18 should be discouraged.

Children must not be added as 'friends' on any Social Network site.

The school will advise parents in terms of their use of Social Networking Sites and how the school will respond to identified issues.

Such as:

- Posting inappropriate comments about staff or children that could be construed as instances of cyberbullying.
- Posting images of children or adults on profiles without permission of the individuals involved, especially if the photographs contain children other than their own.

<u>Protecting Personal Data</u>

- Personal data will be made available to appropriate and approved sources in accordance with the Data Protection Act 2018.

Roles and Responsibilities

Our Computing (and Online Safety leader) is Mrs Mitchell.
Our Computing leader ensures they keep up to date with online safety issues and guidance; keeps the Headteacher, senior leaders and governors updated as necessary; ensures that any online safety concerns are reported, investigated and takes the appropriate action.

Our governor responsible for online safety is Mrs Hayden.
Our governors have an understanding of online safety issues and strategies at the school; are aware of local and national guidance about online safety; are updated at least annually on policy developments.

Our staff responsibilities are to be familiar with the policy and to adhere to its procedures. They should be familiar with the school's policy in regard to:

- Safe use of e-mail.
- Safe use of internet.
- Safe use of school network, equipment and data.
- Safe use of digital images and digital technologies, such as mobile phones, digital cameras and iPads.
- Publication of pupil information/photographs and use of website.
- E-Bullying / Cyberbullying procedures.
- Their role in providing online safety education for pupils.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will always use a child friendly, safe search engine when accessing the internet with pupils (e.g. Google Safe Search – default settings). Staff are to be updated about online safety matters at least once a year.

Managing Internet Access and Other Technologies

Information system security-

- School ICT systems capacity and security will be reviewed regularly.
- All staff and pupils possess individual logons and passwords to the school network with appropriate access rights and privileges.
- Virus protection is installed on all school computers and updated regularly in light of new viruses and Trojan Horses that weaken the school's security.
- Parents' attention will be drawn to the school Online Safety Policy in newsletters, the school brochure and on the school website.
- Parents will be given a copy of the Acceptable Use Policy that their child has signed. They will be strongly encouraged and supported to monitor their children's use of technology at home.
- The school will offer regular online safety sessions for parents.

Glossary

Acceptable Use Policy: A policy that a user must agree to abide by in order to gain access to a network or the internet. In the school's context, it may also cover how other communications services, such as mobile phones and camera phones, can be used on the school premises.

Avatar: A graphic identity selected by a user to represent him/herself to the other parties in a chatroom or when using instant messaging.

Chatroom: An area on the internet or other computer network where users can communicate in real time, often about a specific topic.

Filtering: A method used to prevent or block users' access to unsuitable material on the internet.

Information Literacy: The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.

Instant Messaging (IM): A type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the internet, analogous to a telephone conversation but using text-based, not voice-based, communication.

Spam: Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

Spoofing: Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan Horses: A virus which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.

Virus: A computer program which enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing antivirus software.

Appendices to this Policy

Appendix A – Information Letter to Parents
Appendix B – Acceptable Use Agreement – Parents & Pupils
Appendix C – Acceptable Use Agreement – Workforce

APPENDIX A

ICT Acceptable Use Policy (AUP) – Parent's Letter

Dear Parent/Carer,

The use of ICT including the internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network Sites that incorporate age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider school Online Safety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school.

Along with addressing online as part of your child's learning, we will also be holding a parental online safety awareness session during the school year, and I would take this opportunity to strongly encourage your attendance wherever possible. Further information will be communicated as soon as dates are confirmed.

If you have any concerns or would like to discuss any aspect of the use of ICT in school please contact Mrs Mitchell, our Computing leader.

Yours sincerely

Mrs L Clarke
Headteacher

Appendix B
ICT Acceptable Use Policy (AUP) – Children

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should be entitled to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure that:

- our pupils will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use,
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk, and
- parents and guardians are aware of the importance of e-safety and are involved in the education and guidance of young people regarding on-line behaviour.

These rules reflect the content of our school's online safety policy. It is important that parents/carers read, understand and agree to the following statements in order for their child(ren) to follow the school rules on using ICT, including use of the internet.

Typical classroom online rules for EYFS/KS1

Our Golden Rules for Staying Safe with ICT

- ✓ We only use the internet when a trusted adult is with us.
- ✓ We are always polite and friendly when using online tools.
- ✓ We always make careful choices when we use the Internet.
- ✓ We always ask a trusted adult if we need help using the Internet.
- ✓ We always tell a trusted adult if we find something that upsets us.

Typical classroom online for KS2

Our Golden Rules for Staying Safe with ICT

- ✓ We always ask permission before using the Internet.
- ✓ We only use the Internet when a trusted adult is around.
- ✓ We immediately close/minimise any page we are uncomfortable with (or switch off the monitor).
- ✓ We always tell an adult if we see anything we feel uncomfortable with.
- ✓ We only communicate online with people a trusted adult has approved.
- ✓ All our online communications are polite and friendly.
- ✓ We never give out our own, or others', personal information or passwords and are very careful with the information that we share online.
- ✓ We only use programmes and content which have been installed by the school.

Pupil Acceptable Use Agreement

I understand that while I am a member of Rowlands Gill Primary School I must use technology in a responsible way.

- I will ask a teacher or suitable adult if I want to use the computers.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

I have read and understand the above and agree to follow these rules when:

- I use the school systems and devices (both in and out of school).
- I use my own equipment outside of school in a way that is related to me being a pupil of Rowlands Gill Primary School e.g. communicating with other pupils or teachers, accessing school email, website etc.

Pupil name: _____ Class: _____

Pupil signature: _____ Date: _____

Parent or Guardian Permission

As the parent of guardian of the above pupil, I give permission for my child to have access to the internet and to ICT systems at school.

I know that my child has signed this Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.

I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Parent / guardian name: _____ Signature: _____

Date: _____

This AUP must be signed and returned to school before any access to the school systems is allowed.

APPENDIX C ICT Acceptable Use Policy (AUP) – Workforce

ICT and the related technologies such as e-mail, the internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all of our workforce are aware of their individual responsibilities when using technology. All members of our workforce are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the headteacher.

Introduction and Scope
The Acceptable Use Policy includes accessing cloud services on personal devices and governs the use of Rowlands Gill Primary School's corporate network and cloud-based systems that individuals use on a daily basis in order to carry out business functions.

This policy applies to all employees, governors or trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the school.

This policy should be read in conjunction with the other policies in our information governance policy framework, including the Data Protection policy, Information Security policy and Safeguarding policy.

Email and Internet Use
We provide email accounts and internet access to the workforce to assist with performance of their duties. We also allow the workforce to use its instant messaging service. For the benefit of doubt Instant Messages are classed as email communications in this policy.

Personal Use
Whilst email accounts and the internet should primarily be used for business functions, incidental and occasional use in a personal capacity may be permitted so long as:

- Personal messages or internet usage do not tarnish our reputation, or infringe on business functions,
- Users understand that emails sent to and from corporate accounts are the property of the school,
- Users understand that we may have access to their email account and any personal messages contained within,
- Users understand that we may have access to their internet browsers and browsing history contained within,
- Users understand that emails sent to or from their email account may have to be disclosed under Freedom of Information and/or Data Protection legislation,
- Users understand that we reserve the right to cleanse email accounts at regular intervals which could result in personal emails being erased from the corporate network,
- Users understand that we reserve the right to suspend internet access at any time.

Inappropriate Use
We do not permit individuals to send, forward, or solicit emails, or use the internet in any way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

- Sexually explicit or pornographic messages, images, cartoons, jokes or movie files,
- Unwelcome propositions, profanity, obscenity, slander, or libel,
- Any messages or content containing ethnic, religious, political, or racial slurs,
- Any messages or content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.

Users are also not permitted to use the internet in a way which could affect usage for others. This means not streaming or downloading media files and not using the internet for playing online games.

Other Business Use
Users are not permitted to use emails or the internet to carry out their own business or business of others. This includes, but is not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case-by-case basis at the discretion of school management.

Security
Users will take care to use their email accounts and the internet in accordance with our Information Security policy. In particular users will:

- Use multi-factor authentication where required
- Not click on links from un-trusted or unverified sources,
- Use secure email transmission methods when sending personal data,
- Not sign up to marketing material that could jeopardise our IT network,
- Not send excessively large email attachments without authorisation from management and our IT provider.

Group Email Accounts
Users may also be permitted access to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to suspension of a user's email rights.

The Headteacher will have overall responsibility for allowing access to group email accounts but this responsibility may be devolved to other individuals.

We may monitor and review all email traffic that comes to and from individual and group email accounts.

Social Media Use
We recognise and embrace the benefits and opportunities that social media can contribute to an organisation. We also recognise that the use of social media is a data protection risk due to its open nature and capacity to broadcast to a large amount of people in a short amount of time.

Corporate Accounts
We may have a number of social media accounts across multiple platforms. Nominated users will have access to these accounts and are permitted to post general information about the school. Authorised users will be given the usernames and passwords to these accounts which must not be disclosed to any other individual within or external to the organisation. The Headteacher will have overall responsibility for allowing access to social media accounts.

Corporate social media accounts must not be used for the dissemination of personal data either in an open forum or by direct message. This would be a contravention of our information governance policies and data protection legislation.

Corporate accounts must not be used in a way which could:

- Tarnish our reputation,

- Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs,
- Be construed as sexually explicit,
- Be construed as political beliefs or commentary.

Personal Accounts
We understand that many users will use or have access to personal social media accounts. Users must not use these accounts:

- During working hours,
- Using corporate equipment,
- To conduct corporate business,
- To contact or approach our clients, customers, or partners.

Telephone and Video Conferencing Use (including TEAMs)
We provide users with access to telephone and video conferencing services to assist with performance of their duties.

Inappropriate Use
We do not permit users to use the telephone or video conferencing services in any way which may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

Other Business Use
Users are not permitted to use these services to carry out their own business or business of others. This includes work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case-by-case basis at the discretion of school management.

Accessing Cloud Services on Personal Devices

Introduction
As remote working continues to develop, there has been a move by many organisations to transfer their locally held data into the cloud, enabling access by any internet connected device, anywhere in the world. This brings many benefits to the school, including being able to access data promptly, on a device of their own choice.

However, with this enhanced access comes a high level of risk that the school needs to consider and mitigate through the use of technical controls, expected behaviours and supporting policies. This policy aims to provide the framework for adequate management of the risks posed should users access school systems through a non-school provided device.

Personal Devices
We identify a personal device as any electronic device that has not been provided by us and can be used to access and process personal data, including data accessed from the cloud through an internet connection. This includes, but it not limited to:

- Laptop or PC
- Notebook
- iPad or tablet
- Smartphone

Use of the device must be limited to the individual user, and not be shared resources (e.g. a family device unless each family member has their own password protected profile on it).

Permitted Activity
Whilst using their own devices, users are permitted to access, review and process personal data within the school system in which it is held. Users must only access data they are entitled to in order to fulfil their duties.

It is not permitted for any school data to be downloaded and saved onto any personal device under any circumstances. All school data must remain within the defined systems to ensure it remains secure, available to all authorised personnel and held within our records management system for its full lifecycle, including secure destruction in line with our retention schedule.

By retaining data within school-controlled systems, in the event of an individual exercising their rights as detailed in the UK GDPR; particularly with the right to access (Subject Access Request), the searching criteria to meet a request will not require users to search their own devices for evidence of personal data that may have been stored.

Printing of any personal data to home printers is strictly forbidden. The storage and confidential disposal of paper documents cannot be easily managed and guaranteed when taken off the school site.

Device Security

Anti-virus and Software Security Patching
The range of devices currently available all present different levels of ability to apply appropriate security and protection to the equipment. It is therefore the responsibility of the user to ensure that all available protection and security is applied. Specialist advice should be sought where appropriate.

We require that any device used for accessing school systems in the cloud must have adequate anti-virus software. The software should be installed, configured and maintained by a suitably qualified or experienced person. All available updates must be applied in a timely manner.

Out of date software (including operating systems) can provide vulnerabilities that can be exploited by unscrupulous hackers. All software installed on devices that is going to be used to access school data must be operating at the most up to date version with all security releases applied. All software should be configured and maintained by a suitably qualified or experienced person for the full period that they are used to access school data.

Password/PIN Protection
All devices must be secured by a unique password or security pin to ensure that access to the device is limited to the named user permitted to access the school's personal data. Devices that lack the ability to enforce this level of security must not be used to access school data.

Data on personal devices is unlikely to be encrypted, and therefore particularly vulnerable if lost or stolen. Having a robust password or PIN in place provides an additional layer of protection.

Personal Applications (apps)
Users are asked to be mindful of the apps installed on personal devices that are used to access school data. Some of these apps may have enhanced privileges and tracking within them that monitor use of the device and other items that are being accessed. This should be detailed in the application's terms and conditions and the user should seek assurance that this risk is being effectively managed.

Equipment Disposal
When a device being used to access school information is disposed of, it is the responsibility of the user to ensure that no records or school data have found their way onto the device, either accidently or for a temporary purpose, prior to surrendering it as a part of an upgrade process, at point of resell or for permanent disposal through the WEEE (Waste Electronic and Electrical) process. Specialist advice should be sought where appropriate.

Physical Security
Users should ensure any device used to access school data is kept safe and secured to prevent theft or damage. This includes actions such as not leaving devices overnight in cars, unattended in public spaces, or transported without sufficient protection to prevent accidental damage.

System and Accounts Security
When accessing data held in the cloud via an internet connection (e.g. Microsoft 365), users must ensure that their account is closed when not in use by logging out of the system. It is not permitted for accounts to be left open when not in use, if accessing school systems.

Users are responsible for ensuring any internet connection used to access school data is secured through the use of access controls, such as using a designated username and password. Unsecured network connections (Wi-Fi or hot spots) must not be used, and devices must be configured to prevent automatic connection to unknown networks (e.g. cafes, shopping centres, library etc.).

Data Breaches
In the event of a data breach users must follow the process detailed in the Information Security policy and report any suspected breach immediately.

Users are asked to be mindful of the following situations in which the risk of a data breach increases:

- Systems not shut down appropriately when not in use, leading to unauthorised access of school data.
- Personal devices shared with family, friends, or partners leading to unauthorised access of school data.
- Documents and files are downloaded onto shared devices, and then become accessible to other users of the device.
- Passwords or security PINs are shared with others (e.g. family and partners) leading to unauthorised access of school data.
- Inadequate management of security and software updates leaves a vulnerability to a virus or hack. Once unauthorised control of a device is established it is difficult to identify and remove.
- Disposal of devices that have not been adequately assessed and the permanent removal of any school related data prior to surrender.

Authorised Access
Access to school systems using personal devices is only permitted whilst the user has authorisation to do so. In the event that the user leaves the employment of the school; or the relationship terminates for third parties and contractors; access should not be attempted. To do so would be treated as a data breach and investigated as such. It is a criminal offence under Section 170 of the Data Protection Act 2018 to knowingly access data that you are not entitled to or after you have left our employment.

Exemption Process
An exemption to any element of this policy can only be authorised by the school's Senior Information Risk Owner (SIRO) – The Headteacher. Authorisation will only be given where there is a clear business need and following a full risk assessment to ensure risks are mitigated.

Workforce Acceptable Use Agreement

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in online safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of the Computing leader.
10. I will ensure that personal data (including data held on Arbor) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
13. I will report any known misuses of technology, including the unacceptable behaviours of others.
14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
16. I have a duty to protect passwords and personal network logins and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's online safety policy and help children to be safe and responsible in their use of ICT and related technologies.
20. I understand that these rules are designed for the online safety of all users and that if they are not followed, school sanctions will be applied, and disciplinary action taken.

User Signature

I have read the Workforce Acceptable Use Policy and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature: ……Date: ……

Full Name: …….. (PRINT)

Position/Role: ……