Rothwell Primary School
Acceptable Use and
Online Safety Policy

Based on the **Leeds City Council guidance for Staff working in Educational Settings on the Use of Digital Technologies and Social Media** (2019) written by Leeds Children's Services.

Agreed by the Resources sub-committee	**July 2022**
Renewal Date	**July 2023**

Caroline Taylor (Computing Leader)

Lindsey Bown (SENCO and Designated Safeguarding Teacher)

Paul Durkan (Deputy Head and Designated Safeguarding Teacher)

Working together to

our potential.

CONTENTS **Page**

Section 1 - Overview

ICT and the internet are essential tools for teaching and learning and communication that are used in Rothwell Primary to deliver the curriculum, and to support and challenge the varied learning needs of its students. ICT is used to share information and ideas with all sections of the school community. Rothwell Primary School encourages the use of school Computing facilities for the mutual benefit of all its staff and pupils. Similarly, the regulations that constitute this policy seek to provide for the mutual protection of Rothwell Primary School and the rights of its staff and pupils.

At Rothwell Primary the use of the internet and ICT is seen as a responsibility and it is important that students and staff use it appropriately and practise good online safety. It is also important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

E safety covers the use of the internet as well as mobile phones, electronic communications technologies and the use of social media and social networks. We know that some adults will use these technologies to harm students. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. Staff have a duty of care to protect children from risk of harm, as well as a duty to ensure their own conduct does not bring into question their suitability to work with children.

This guidance takes into account the principles of the Safer Working Practice Guidance (National Safer Recruitment Consortium) as well as guidance from the Department for Education (Safeguarding Children in a Digital World), CEOP (Child Exploitation and Online Protection) and Communication Act 2003 (Section 127 Improper Use of Public Electronic Communications Network).
http://www.legislation.gov.uk/ukpga/2003/21/section/127

This policy may be updated or supplemented by specific standards or procedures to reflect further developments in technology or legislation or other relevant changes. This policy should be used in conjunction with the school's Child Protection Policy, Anti-Bullying Policy, Computing Policy and Staff Disciplinary Policy.

This guidance applies to all staff employed either directly or indirectly by Rothwell Primary as well as volunteers and staff not employed directly by the school but based at the school. All staff are expected to adhere to this code of practice to ensure the safety of the students, young people and adults at risk who they may come into contact with through their professional role. Any member of staff found to be suspected of any breach of these guidelines may be subject to disciplinary action in accordance with the Schools Disciplinary Policy and Procedure.

The Computing Leader and Safeguarding team will attend regular training (no longer than every two years) and this training will be fed back appropriately to all members of the school community to ensure that it is embedded in the ethos of the school.

1.1 Definition of Students:

Throughout this document references are made to students. For the purpose of this document this term refers to all children, young people and adults at risk in educational settings whom a professional may come into contact with, as a direct result of their professional role.

1.2 Adults at Risk: means adults who need community care services because of mental or other disability, age or illness and who are, or may be unable, to take care of themselves against harm or exploitation. The term replaces "vulnerable adults".

Section 2 - Responsibilities

Governors and Head Teachers are responsible for ensuring this guidance is shared with and adhered to by all staff.

Staff are responsible for their own actions and must act, and be seen to act, in the best interests of children at all times. Staff must ensure they understand and adhere to this guidance as well as Rothwell Primary's code of conduct and Internet Acceptable Use Policy. Staff are responsible for acting promptly to prevent and safeguard children from potential abuse online and for reporting any concerns in accordance with the Leeds Childrens Services Safeguarding & Child Protection Policy for Schools and Colleges.

Staff are solely responsible for any content on their own personal social media networks and electronic devices. This means that staff are responsible for managing their own applications and content to ensure that it does not breach the school's safer working practice guidance, or undermine public confidence in the school or the education profession. Staff are personally responsible for security and privacy settings when using social media via their chosen equipment and as such failing to ensure adequate and appropriate settings are in place may lead to disciplinary action should the content be found to breach school expectations of professional conduct by bringing the school into disrepute.

Staff are also responsible for ensuring their own use of ICT and social media is professional and appropriate at all times. Staff must be aware that their conduct online, both inside and outside of school, must not breach the school's code of conduct or professional expectations. Any behaviour that is deemed to breach such expectations may be subject to disciplinary action.

The Management Team (SLT) accepts the following responsibilities:

- Ensure adequate technical support is in place to maintain a secure Computing system (company: Primary ICT support)
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets
- Ensure liaison with the Governors
- Develop and promote an E-Safety culture within the school community
- Ensure that all staff and pupils agree to the Acceptable Use Policy and that new staff have E-Safety included as part of their induction procedures
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to E-Safety
- Receive and regularly review E-Safety incident logs; ensure that the correct procedures are followed should an E-Safety incident occur in school and review incidents to see if further action is required
- Take ultimate responsibility for the E-Safety of the school community

Responsibilities of the Computing Leader

- Promote an awareness and commitment to E-Safety throughout the school
- Create and maintain E-Safety procedures within school
- Develop an understanding of current E-Safety issues, guidance and appropriate legislation, attending regular training for updated guidance
- Ensure delivery of an appropriate level of training in E-Safety issues
- Ensure that E-Safety education is embedded across the curriculum
- Ensure that E-Safety is promoted to parents and carers
- Ensure that any person who is not a member of school staff, who makes use of the school Computing equipment in any context, is made aware of this Acceptable Use and E-safety Policy
- Monitor and report on E-Safety issues to the Leadership team and Governors as appropriate
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable
- Ensure that good practice guidelines for E-Safety are displayed in classrooms and around the school

Responsibilities of all Staff

- Read, understand and help promote the school's E-Safety guidance
- Read, understand and adhere to this staff Acceptable Use and E-Safety Policy
- Take responsibility for ensuring the safety of sensitive school data and information

- Develop and maintain an awareness of current E-Safety issues and legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Ensure that personal social network pages are secured from general view and that content does not bring the school or themselves into disrepute
- Do not mention the name of the school on social networking sites including as part of their profile
- Take ultimate responsibility for the content and comments on their personal Social Media sites and pages
- Embed E-Safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all E-Safety incidents that occur in line with Safeguarding policy.
- Respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Report any computing equipment issues using the Primary ICT Support 'Request Support' facility, alerting the school admin and Computing Subject Leader to this also.

Additional Responsibilities of Technical Staff (service through Primary ICT Support)

- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps are in place to safeguard the security of the school Computing system, sensitive data and information. Review these regularly to ensure they are up to date
- At the request of the Leadership team, conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use and E-safety Policy is being followed
- Report any E-Safety related issues that come to their attention to the Headteacher and/or designated safeguarding team
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems
- Ensure that suitable access arrangements are in place for any external users of the school computing equipment
- Liaise with the Local Authority and others on E-Safety issues

Responsibilities of Pupils

- Understand and adhere to the Pupil Acceptable Use and follow all safe practice guidance
- Take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks

posed by the personal technology owned and used by them outside of school

- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home

Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening

- Report all E-Safety incidents to appropriate members of staff
- Discuss E-Safety issues with family and friends in an open and honest way

Responsibilities of Parents and Carers

- Help and support the school in promoting E-Safety
- Read, understand and promote the Pupil Acceptable Use Policy with their children
- Discuss E-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's E-Safety policies and guidance as part of the schools overarching safeguarding procedures
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-Safety awareness
- Ensure appropriate funding and resources are available for the school to implement their E-Safety strategy

Section 3 - Social Contact with Students

Staff must not establish or seek to establish social contact with students, for the purpose of securing a friendship or to pursue or strengthen a relationship. Even if a student themselves seeks to establish social contact. If this occurs coincidentally, the member of staff should exercise their professional judgement in making a response and be aware that such social contact could be misconstrued. Staff should alert the Headteacher of any such contact immediately as part of safeguarding of children.

Contact with students should be through appropriate channels at all times and should be within clear and explicit professional boundaries. This means staff should only contact students in the school setting, using school equipment and regarding school matters, with appropriate permission from senior leadership.

Staff should not give, nor be required to give, their personal details such as home or mobile number, social media identities or personal email addresses to students. Any member of staff found to be in contact with students through any of the above means, or any other unapproved method, without prior consent of the head teacher/senior leaders may be subject to disciplinary action.

Internal email and approved contact systems should only be used in accordance with the appropriate ICT policy and/or Acceptable Use policy.

Section 4 - Social Media

In order to make best use of the many educational and social benefits of new and emerging technologies, pupils need opportunities to use and explore the digital world. Online risks are posed more by behaviours and values than the technology itself.

Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies, which detail how new and emerging technologies may be used.

Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand-held devices. (Given the ever-changing world of technology, it should be noted that this list gives examples only and is not exhaustive.)

Staff should not have contact with students using social media, and specifically social networking sites without prior permission of the Headteacher. Staff must not add students as friends or respond to friend requests from students. If a member of staff suspects that an existing friend is a student, child or young person, they must take reasonable steps to check the identity of the individual, report this to the Headteacher as a safeguarding issue, and end the social media friendship.

It is recognised that personal access to social networking sites outside the work environment is at the discretion of the individual. However, members of staff should consider their use of social networks as they take on the responsibilities of a professional, taking particular care to secure personal information and ensure their use of such networking sites is respectable and appropriate at all times.

Secure and suitable strength passwords should be devised and security settings should be applied to access your profile and the information contained within it,

so that your profile is limited to those explicitly given access. Users should not sign up to non-work-related web-accounts using a work email address or password.

It is also advisable to log out of any sites on a personal computer or an application on a mobile device to ensure maximum security. Activities undertaken by others who can have access to your social media platforms shall be deemed attributable to the user logged in at the time, unless there is a good and verifiable reason to suspect otherwise (e.g. hacking).

Understand and check your privacy settings on your social media profiles so you can choose to limit who has access to your data. You may also want to consider how much personal information you include on your profile.

Personal profiles on social networking sites and other internet posting forums should not identify your employer or place of work and careful consideration should be given to information which is published on such sites. For example, information which is confidential, damaging to the school or undermines public confidence in the school's reputation.

All postings to social media websites should be considered in the public domain. Therefore, only post comments, videos and pictures, which you would be happy to share with any group of friends, strangers or colleagues. Do not post information which could lead to the identification of someone connected to the school or your profession without their explicit consent. This includes posting images of people. Remember once you have published information you cannot guarantee it can be fully removed, and you cannot control how it is shared.

Material published by staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of a student, colleagues or member of the school community will be dealt with under the disciplinary procedure.

Subject to the constraints within this policy it is understood that employees have the right to free expression of opinion in their lives outside school, including on matters of public policy.

Section 5 - Images of Students through Video or Photography

Many work based activities involve recording images and these may be undertaken as part of the curriculum, extra school activities, for publicity, or to celebrate achievement. However, written explicit consent must be gained from legal guardians as well as senior management prior to creating any images of students.

Using images of students for publicity purposes requires the age-appropriate consent of the individual concerned and their legal guardians. Images should not be displayed on websites, in publications or in a public place without such consent. The definition of a public place includes areas where visitors to the school or service provision have access. Consent to use images can be withdrawn at any time, without giving a reason, and in such cases, staff must make every effort to remove/destroy these images wherever they have been published.

Photograph or video images must be created using equipment provided by the work place. It is not acceptable to record images of students on personal equipment such as personal cameras, mobile phones or video camera. Images of students must not be created or stored for personal use.

Members of staff creating or storing images of students using personal equipment without prior consent will be subject to disciplinary action.

Members of staff must:

- be clear about the purpose of the activity and about what will happen to the photographs when the lesson/activity is concluded;
- ensure that senior management is aware that photography/image equipment is being used and for what purpose;
- ensure that all images are available for scrutiny in order to screen for acceptability;
- be able to justify images of students in their possession;
- ensure that images are held only for as long as necessary for the 'purpose';
- avoid making images in one to one situations.

Members of staff must not take, display or distribute images of students unless they have explicit written consent to do so. Failure to follow any part of this code of practice may result in disciplinary action being taken.

For further guidance on creating, displaying and storing images of students please refer to the Safer Working Practice Guidance (National Safer Recruitment Consortium 2019) as well as guidance from the Department for Education (Safeguarding Children in a Digital World) and CEOP (Child Exploitation and Online Protection).

Published content and the school web site

- The contact details on the Web site should be the school admin address, e-mail and telephone number.
- Staff or pupils' personal information will not be published. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs. Pupil's work can only be published with the permission of the parents.

Social networking and personal publishing

- The school will block/filter access to social networking sites. These will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Photographs, Videos, and Indecent images

Below are the specific expectations for the use of photographic materials from the document "Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings" DSCF 2009

Working with pupils may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well being of pupils. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose.	**This means that adults should:** • be clear about the purpose of the activity and about what will happen to the images when the activity is concluded • be able to justify images of children in their possession • avoid making images in one to one situations or which show a single child with no surrounding context

Careful consideration should be given as to how activities involving the taking of images are organised and undertaken. Care should be taken to ensure that all parties understand the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media, or on the Internet. There also needs to be an agreement as to whether the images will be destroyed or retained for further use, where these will be stored and who will have access to them. Adults need to remain sensitive to any children who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings. It is not appropriate for adults to take photographs of children for their personal use. **It is recommended that when using a photograph the following guidance should be followed:** • if the photograph is used, avoid naming the pupil • if the pupil is named, avoid using their photograph	• ensure the child/young person understands why the images are being taken and has agreed to the activity and that they are appropriately dressed. • only use equipment provided or authorised by the school • report any concerns about any inappropriate or intrusive photographs found • always ensure they have parental permission to take and/or display photographs **This means that adults should not:** • display or distribute images of children unless they have consent to do so from parents/carers • use images which may cause distress • use mobile telephones or any other similar devices to take images of children take images 'in secret', or taking images in situations that may be construed as being secretive

• schools should establish whether the image will be retained for further use • Images should be securely stored and used only by those authorised to do so.	
There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with pupils, if proven. Adults should not use equipment belonging to their school/service to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children. Adults should ensure that pupils are not exposed to any inappropriate images or web links. School/service and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. E.g. personal passwords should be kept confidential. Where indecent images of children or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.	**This means that schools/services should** • have clear E-Safety policies in place about access to and use of the internet • make guidance available to both adults and pupils about appropriate usage. **This means that adults should:** • follow their school/service's guidance on the use of IT equipment • ensure that children are not exposed • to unsuitable material on the internet ensure that any films or material shown to pupils are age appropriate

Section 6 - Use of personal technology/equipment in school

- The use of any personal equipment in schools should always be with the prior permission of senior management in order to comply with health and safety regulations, safer working practice guidance, data protection and school policies. Members of staff should take care to comply with acceptable use and ICT policies.

- Personal equipment capable of recording images, moving images or sounds and those used for accessing the internet such as mobile phones, cameras, video cameras and laptops should not be used in work time without the prior permission of senior management.

- Any member of staff found to be using such personal equipment without prior authorisation may be subject to disciplinary action in accordance with the Schools Disciplinary Policy and Procedure.

- No photographs or videos of school activities and/or pupils are to be taken and/or stored on personal mobile phones or computers.

- All photos are to be stored centrally on the school network, SharePoint or Google-drive.

- Pupil mobile phones will be switched off and kept in the school office in line with school safeguarding policy.

- Staff will be issued with a school phone where contact with pupils/parents is required e.g. school residential visits/trips.

Section 7 - Internet Use

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.

- Internet use will enhance learning
- 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.
- Pupils will be educated 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

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Members of staff must follow and adhere to the policies on the use of IT equipment at all times and must not share logins or password information with other members of staff, students, children or young people, friends, family or members of the public.

As a general principle, internet access is provided to employees to support work related activities. The following list is not intended to be an exhaustive list, but sets out broad areas of use that the school considers to be acceptable uses of the internet.

Managing Internet Access, E-mail and Google Classroom

- Virus protection will be updated regularly (Usually daily- automatically over the school network)
- Pupils may only use approved e-mail accounts on the school system (closed network), with email facility switched off when not being taught explicitly (managed by Primary ICT Support). Pupils may share work through Google Classroom 'Share' button within the closed network.
- Pupils must immediately tell a teacher if they receive offensive e-mail or document.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation will only be by staff and should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Google Classroom may be set to allow pupils to comment on staff posts on the stream, but not post directly themselves. Pupils can be blocked from commenting at any time by all staff members of the classrooms; pupils will be blocked from commenting if not doing so appropriately, in line with the school behaviour policy.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The school admin and Primary ICT Support will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

7.1 Acceptable Use

- To provide communication within the school via school email or the school website
- To provide communication with other schools and organizations for educational purposes
- To set and manage school-related home-learning tasks online

- To distribute details regarding school meetings
- To provide electronic methods of communication
- Any other use that directly supports work related functions.

7.2 Unacceptable Use

The following uses will be regarded as not acceptable irrespective of the means of internet access:

- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Use for racial, sexual, homophobic or other harassment.
- To access pornographic, obscene or illegal material.
- To solicit personal information with the intent of using such information to cause emotional or physical harm.
- Entering into a commitment on behalf of the school (unless you have explicit permission to do this).
- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material.
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised areas.
- Publishing defamatory and/or knowingly false material about Rothwell Primary, your colleagues and/or our pupils on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
- Revealing confidential information in a personal online posting, upload or , transmission, including financial information and information relating to our pupils, staff and/or internal discussions
- Use of personal email to communicate with or about any (name of school) students
- Introducing any form of malicious software into the corporate network
- To disrupt the work of other users, for example, includes the propagation of computer viruses.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access where reasonable steps/systems by the school have been put in place to prevent such access.
- The school will audit Computing provision to establish if the E-Safety policy is adequate and that its implementation is effective.

Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school Child Protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Where necessary, discussions will be held with the Police to establish procedures for handling potentially illegal issues.

Introducing the E-Safety policy to pupils

- E-Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored. The new Computing Scheme of Work (2016) has specific E-Safety content that must be delivered to each year group.
- Staff and the E-Safety policy
- All staff will be given access to the School E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Enlisting parents' support
- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure, parental workshops and on the school Web site.

Protecting Individual User Profiles

- It is the responsibility of all users issued with a computer username and password to keep these details secret. It is essential that strong passwords are used (At least 8 characters, containing at least a capital and a numeral, without personal information). Passwords must be changed regularly to maintain security. Occasionally, Primary ICT Support may implement a forced password change across the site; notifications and scheduling of this will be managed through the school admin team.
- Teaching staff with laptops should ensure that they enable a screensaver that requires staff to re-enter their passwords before regaining access to the system. Laptops should be set up so that closing the lid makes the computer 'sleep' this option also requires a password when is restarted. Where laptops are to be used for displaying content on an Interactive Smart Board, the screensaver can be temporarily disabled and enabled again once finished.
- Staff must ensure that their laptop/workstation is locked before leaving it unattended. This is especially important due to the access to sensitive data, pupil data, personal data and SIMS data that could be achieved by leaving a computer unsecured. Users are required to ensure that personal/sensitive data is kept securely as per the provisions of the Government Data Protection Act 2018.

- To access the school network and Google Drive, the youngest members of the school (FS/KS1) will be issued with generic passwords that are easy for them to use and remember.
- As pupils move into KS2, pupils are required to use a personalised and unique password to access these. A secure copy of the Google passwords will be kept by SLT LKS2 and UKS2 Phase Leaders and Computing Leader (to aid the resetting of forgotten passwords); network passwords are maintained and reset by Primary ICT Support. Pupils must keep their passwords secret; this is reinforced during E-Safety lessons.

Section 8 - Confidentiality and Security

- The storing and processing of personal information is governed by the General Data Protection Regulation and Data Protection Act 2018. Employers are required to provide clear advice to staff about their responsibilities under this legislation so that, when considering sharing confidential information, the principles set out in the legislation apply.

- Members of staff may have access to confidential information about students and families and the organisation in order to undertake their everyday responsibilities and in some circumstances this may be highly sensitive or private information. Such information should only be shared when legally permissible to do so and in the interest of the child. Records should only be shared with those who have a legitimate professional need to see them.

- Only authorised school based devices and systems should be used to store and transfer confidential information. Developments in technology have improved the security of email. This has meant that Leeds City Council have been able to follow centrally issued guidance to protect personal and special category data sent by standard email. When email services are configured appropriately at BOTH ends of the route, email is just as good as Mail Express or any other secure data transfer mechanism once controls are in place.

- For further guidance in relation to sending personal information electronically, please refer to the guide for schools – December 2018 titled ‘Exchanging data electronically’. Members of staff found to be compromising confidentiality by use of unauthorised systems and devices could be subject to disciplinary action.

- For further guidance in relation to confidentiality issues and safe storage of data please refer to the Safer Working Practice guidance document (2019).

Computing facilities

- Access to school Computing facilities is managed by an appointed Computing Network Manager (Primary ICT Support). Use of any of Rothwell Primary School’s Computing facilities is at the discretion of Rothwell Primary School.

- The phrase ‘Computing Facilities’ as used in this policy shall be interpreted as including any computer hardware or software owned or operated by Rothwell Primary School and any allocation of time, memory, disk space or other measure of space on any of Rothwell Primary School’s hardware, software or networks

Ownership

- Computing facilities owned by Rothwell Primary School and software and/or data developed or created (for whatever reason) on that equipment remains in all respects the property of Rothwell Primary School. The Patents Act 1977 and the Copyright, Designs and Patents Act 1988 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the employer.

Desktop PCs

- Desktop PCs are a critical asset to Rothwell Primary School and must be managed carefully to maintain security, data integrity and efficiency. Users must consult Primary ICT Support before installing any additional software on computers managed by Primary ICT Support.
- All users have access to appropriate areas on Rothwell Primary School’s file servers for the secure storage of valuable files. Valued documents and files should not be stored on Desktop PCs. Files stored on Desktop PCs are at risk of loss through hardware/software failure or automated administrative activity.
- Desktop PCs include the CPU/hard-drive unit and monitor both of which are subject to change.

Laptop PCs (including Chromebooks)

- Laptop PCs are at high risk from loss or theft and require additional security protection. All reasonable precautions must be taken to ensure that hardware is stored securely. Also, to protect the integrity of Rothwell Primary School systems and data procedures, passwords or authentication devices for gaining remote access to Rothwell Primary School systems must not be stored with the computer. This includes the saving of passwords into remote access software.
- Laptops from the ‘trolley banks’ should be returned to these by staff and checked at the end of each session
- Highly confidential data can be encrypted to protect it in the event of Laptop PC loss.
- Primary ICT Support can help with this process.
- If your Laptop PC is lost or stolen Primary ICT Support must be notified as soon as possible and a report made to the police.

Handheld and Mobile Devices

- Handhelds and mobiles, including ipads/ipod touch, are at high risk from theft due to their size and nature of usage. Loss of the device can expose Rothwell Primary School to a large liability through fraudulent use. It is therefore vital that staff are vigilant in caring for their security.

- Rothwell Primary School should take care to keep these devices concealed when not in use and to be conscious of onlookers who may be targeting devices for theft. In the event that a device is stolen, Rothwell Primary School will be expected to report the theft to the police, obtain an incident number and contact Primary ICT Support as soon as possible

Loan Equipment

- Policy regarding loan equipment is similar to that for laptops and handheld or mobile devices. Most loan equipment is highly portable and attractive to thieves. Users who borrow loan equipment sign for it and bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use.
- If loan equipment is stolen or lost, Primary ICT Support should be informed immediately. It may also be that the user responsible for its care has to report the theft to the police and report the incident number to School ICT.
- Any member of staff wishing to borrow equipment should seek permission from the head teacher or school admin beforehand and must complete details in the loan register, kept in the School Admin Office.

Data Security

- You must only access information held on Rothwell Primary School's computer systems if you have been properly authorised to do so and you need the information to carry out your work. Under no circumstances should you disclose personal or other confidential information held on computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.
- It is school policy to store data on a network drive where it is regularly backed up. You must ensure that data that is not stored on the network file server is regularly backed up.

Personal Data and the Data Protection Act

- Rothwell Primary School maintains a notification to the Data Protection Commission in compliance with the Data Protection Act 1998. This notification is held on a public register and contains details of the Agency's holding and processing of personal data.
- It is the responsibility of all Rothwell Primary School staff to ensure that personal data is held and processed within the terms of Rothwell Primary School's notification and in compliance with the data protection principles.
- Personal data shall be:
    - obtained processed fairly and lawfully
    - held for specified lawful purpose(s)
    - not used or disclosed in a way incompatible with the purpose(s)
    - adequate, relevant and not excessive for the purpose(s)
    - accurate and up to date
    - not kept longer than necessary

- available to the data subject
- Kept secure.
-

- Rothwell Primary School should note that all data and correspondence, including email messages, held by Rothwell Primary School may be provided to a data subject, internal or external, in the event of a subject access request.

Section 9 - Cyber Bullying

- All forms of bullying, including cyber bullying, are taken very seriously. Bullying is never tolerated and it is not acceptable for any member of staff to behave in a manner which is intimidating, threatening or in any way discriminatory. Behaviour which constitutes Bullying or Harassment may be dealt with under the Leeds Grievance/Bullying and Harassment Policy and could result in disciplinary action.

- However, this doesn't just extend to behaviour within the work place. In some instances bullying or harassment that occurs outside the workplace where there is a link to employment could also fall under the responsibility of the employer and therefore result in disciplinary action being taken against the responsible individual.

- Certain activities relating to cyber bullying could be considered criminal offences under a range of different laws. Cyber bullying consists of threats, harassment, embarrassment, humiliation, defamation or impersonation and could take the form of general insults, prejudice based bullying or discrimination through a variety of media. Media used could include email, Virtual Learning Environments, chat rooms, web sites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

- If an allegation is received that a member of staff is responsible for comments made online which could be deemed harmful, threatening, defamatory, abusive or harassing in any way towards another employee, the school will investigate this matter. Any allegation of bullying or harassment made by an employee against another member of staff where the accused uses the internet, mobile phone, text message or email, along with any other forms of abuse, may be dealt with through the Grievance/Bullying and Harassment Policy and could lead to disciplinary action.

Staff are required to take steps to protect themselves and their personal information by:

- Keeping all passwords secret and protect access to their online accounts
- Not befriending students and young people on social networking services and sites

- Keeping personal phone numbers private
- Not using personal phones to contact parents, students and young people
- Keeping personal phones secure, i.e. through use of a pin code.
- Not posting information about themselves that they wouldn't want employers colleagues, students, young people or parents to see
- Not retaliating to any incident
- Keeping evidence of any incident
- Promptly reporting any incident using existing school procedures for reporting safeguarding concerns.

Staff in schools, as well as students, may become targets of cyberbullying. Staff should never retaliate to, i.e. personally engage with, cyberbullying incidents. They should report incidents appropriately and seek support via the school safeguarding team.

Staff should report all incidents to the designated safeguarding staff. The designated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.

Further information and advice regarding cyber bullying can be found in the DfE guidance documents Preventing and Tacking Bullying 2017 and Cyberbullying: Advice for Head Teachers and School Staff 2014.
https://www.gov.uk/government/publications/preventing-and-tackling-bullying