Reedley Primary School
Use of Technology Policy

Our school nurtures curiosity and creativity through an inspiring, broad and engaging curriculum, where learning is at the heart of all that we do. Children at Reedley learn to become resilient and self-assured in a safe environment where challenge is key. Team Reedley are encouraged to thrive and achieve as individuals, preparing them for their role as caring and active citizens in modern Britain.
(Mission statement)

Use of Technology Policy
Part One - Internet Acceptable Use Policy
Part Two - E safety Policy
Part Three - Use of Social Networking
Part Four – Guidance for Safer Working Practice

Introduction

Use of computers, tablets and access to the internet is becoming as commonplace as the telephone or TV. Significant educational benefits should result from curriculum technology use, including access to information from around the world and the abilities to communicate widely. Internet safety depends on staff, schools, governors, advisers and parents to take responsibility for the use of the internet.

• The internet is an essential element in 21st Century life for education, business and social interaction. Reedley School has a duty to provide children with quality internet access as part of their learning experience. The purpose of internet use in school is to raise educational standards, to promote pupil achievement and to support the professional work of staff.

• Benefits of using the internet allows access to world-wide educational resources including museums and art galleries, and staff professional reasonable precaution to ensure that users access only appropriate material.

• Rules for internet access will be posted near all computers.

• Virus protection will be installed and updated regularly.

Part One - INTERNET ACCEPTABLE USE POLICY For: Pupils, staff and visitors

1. This policy applies to all staff of Reedley Primary School and to those offered access to school resources. This document, which covers internet, Intranet and e-mail use and which does not form part of the contract of employment, may be subject to amendment from time to time.

2. The internet system (i.e. internet, Intranet and e-mail) is the property of Reedley Primary School and may be subject to monitoring and access by the school at its discretion. All access to the internet and email system is automatically logged.

3. Use of the internet system by school employees is permitted and encouraged where such use is suitable and is in accordance with the goals and objectives of the school. Abuse of such use may lead to disciplinary action being taken.

4. The internet system is to be used in a manner that is consistent with the school's ethos, rules and regulations and as part of the normal execution of an employee's job responsibilities.

5. Generally, the internet system should be used for business purposes. Reasonable personal use is permitted. However, users may be subject to limitations on their use of such resources.

6. The distribution of any information through the internet system is subject to the scrutiny of the school.

The school reserves the right to determine the suitability of this information.

Users shall not:

1.Visit internet sites that contain obscene or other objectionable materials. The accessing or downloading of pornographic material is prohibited and is likely to constitute gross misconduct, which may lead to dismissal.

2.Make or post indecent, demeaning or disruptive remarks, proposals or materials on the internet system.

3.Copy, share, forward or display any material, whether internal or external, that is obscene or defamatory or which is intended or likely to harass or intimidate another person.

4.Disclose any information that is confidential to the school, for example parents' personal details.

5.Represent personal opinions as those of the school.

6.Upload, download or otherwise transmit software or any copyrighted materials belonging to parties outside the school or to the school itself.

7.Download any software or electronic files without implementing virus protection measures that have been approved by the school.

8.Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.

9.Examine, change or use another person's files, output, user name or password for which they do not have explicit authorisation.

10.The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately. The school retains the right to report any illegal violation to the appropriate authorities. Below are the rules for responsible internet and e-mail use which are published around the school.

<u>Rules for Responsible internet and E-Mail Use - pupils</u>

At Reedley School access to the computers, electronic devices and to the internet is a privilege.

The school computers, devices and the internet are primarily used for learning.

These rules will help us to be fair to others and keep everyone safe.

- Failure to follow any of these rules will result in access to the school network being restricted or denied.

- On the school network or school devices, I will only use my personal username and password, which I will keep secret.

- I will not look at or delete other people's files.

PART TWO – E safety Policy

The role of the eSafety Co-ordinator includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's eSafety Policy and associated documents, including Acceptable Use Policies.

- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.

- Ensuring all staff are aware of reporting procedures and requirements should an eSafety incident occur.

- Ensuring the eSafety Incident Log is appropriately maintained and regularly reviewed.

- Keeping personally up-to-date with eSafety issues and guidance through liaison with the

- Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).

- Providing or arranging eSafety advice/training for staff, parents/carers and governors.

- Ensuring the Headteacher, SLT, staff, pupils and Governors are updated as necessary.

- Liaising closely with the school's Designated Safeguarding Lead/Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

At Reedley Primary School the eSafety Co-ordinators are Carley Edwards and Kerry Boocock. The SLT is responsible for dealing with eSafety incidents.

- Staff are aware of the different types of eSafety incident (illegal and inappropriate) and how to respond appropriately.

- Children are informed of relevant procedures through discussions with members of staff.

- Incidents are logged on CPOMS.

- The above mentioned eSafety incidents are monitored on a regular basis and reviewed by the Governing Body

- The SLT will decide at which point parents or external agencies are involved

- The school uses the 'eSafety Incident/ Escalation Procedures' document (See Appendix) as a framework for responding to incidents.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). Staff should never personally investigate, interfere with or share evidence as they may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Any potential illegal content would be reported to the Internet Watch Foundation. They are licensed to investigate - schools are not!

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred More details regarding these categories can be found on the IWF website.

Staff are encouraged to use ICT resources in their teaching and learning activities, to conduct research, and for contact with others on the education world. Electronic information-handling skills are now fundamental to the preparation of citizens and future employees in the information age.

Staff are encouraged to investigate the possibilities provided by access to this electronic information and communication resource, and blend its use, as appropriate, within the curriculum. They should model appropriate and effective use and provide guidance and instruction to pupils in the acceptable use of the Intranet/Internet.

When using the Internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, discrimination and obscenity and all school staff are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the education sector.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful. Files and e-mails stored on the school network are property of the school, not the user.

Staff members are provided with email accounts and passwords to the school network. These passwords must only be used by the account holder. They must not be shared, display or made available to children.

If a staff member feels that their account has been violated, they must report this to the leadership team immediately. Once the employee has left the school’s employment, the accounts will be withdrawn and the user has no rights to access the information held within those accounts. Use of ipads and school issued computers

-School issued computers remain the property of the school

-Members of the leadership team can access any of the devices at any time

-ipads and school issued computers should not be used for social networking purposes. Apps must not be uploaded on the ipads for social networking sites.

-Personal photos should not be taken for personal use using the iPad/camera

-Staff need to take care when opening emails and when accessing websites using the ipads and computers, to minimise the risk of viruses.

If a virus is suspected, this needs to be reported at the earliest opportunity.

Part Three: Use of social Networking

LANCASHIRE COUNTY COUNCIL CHILDREN AND YOUNG PEOPLE'S DIRECTORATE GUIDANCE ON THE USE OF SOCIAL NETWORKING SITES AND OTHER FORMS OF SOCIAL MEDIA

Introduction

The aim of this document is to provide advice and guidance for those working with children and young people in educational settings (including volunteers) regarding the use of Social Networking Sites.

The document has been produced for Governing Bodies and Headteachers of all Schools in Lancashire and for Senior Managers and Management Committees within the County Council's centrally managed teaching services. The document has been the subject of consultation with the recognised Professional Associations and Trade Unions.

Background

The use of social networking sites such as Facebook, Instagram, Snapchat, TikTok, Twitter, Bebo and MySpace is rapidly becoming the primary form of communication between friends and family. In addition, there are many other sites which allow people to publish their own pictures, text and videos such as YouTube, TikTok and blogging sites. It would not be reasonable to expect or instruct employees not to use these sites which, if used with caution, should have no impact whatsoever on their role in school. Indeed, appropriate use of some sites may also have professional benefits. It is naïve and outdated however to believe that use of such sites provides a completely private platform for personal communications.

Even when utilised sensibly and with caution employees are vulnerable to their personal details being exposed to a wider audience than they might otherwise have intended. One example of this is when photographs and comments are published by others without the employees consent or knowledge which may portray the employee in a manner which is not conducive to their role in school.

Difficulties arise when staff utilise these sites and they do not have the knowledge or skills to ensure adequate security and privacy settings.

In addition, there are some cases when employees deliberately use these sites to communicate with and/or form inappropriate relationships with children and young people. Specific Guidance Employees who choose to make use of social networking site/media should be advised as follows:-

• That they familiarise themselves with the sites 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended;

• That they do not conduct or portray themselves in a manner which may:-

• bring the school into disrepute;

• lead to valid parental complaints;

• be deemed as derogatory towards the school and/or it's employees;

• be deemed as derogatory towards pupils and/or parents and carers;

• bring into question their appropriateness to work with children and young people.

• That they do not form on-line 'friendships' or enter into communication with *parents/carers and pupils as this could lead to professional relationships being compromised.

• No reference is made to Reedley Primary School on staff personal on-line account, without permission from the Headteacher

• On-line friendships and communication with former pupils should be strongly discouraged particularly if the pupils are under the age of 18 years. (*In some cases, employees in schools/services are related to parents/carers and/or pupils or may have formed on-line friendships with them prior to them becoming parents/carers and/or pupils of the school/service.

In these cases, employees should be advised that the nature of such relationships has changed and that they need to be aware of the risks of continuing with this method of contact. (They should be advised that such contact is contradictory to the Specific Guidance points above)

Safeguarding Issues
Communicating with both current and former pupils via social networking sites or via other non-school related mechanisms such as personal e-mails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

Communication with Pupils (including the Use of Technology)

In order to make best use of the many educational and social benefits of new technologies, pupils need opportunities to use and explore the digital world, using multiple devices from multiple locations. It is now recognised that that e.safety risks are posed more by behaviours and values than the technology itself.

Adults working in this area must therefore ensure that they establish safe and responsible online behaviours. This means working to local and national guidelines on acceptable user policies. These detail the way in which new and emerging technologies may and may not be used and identify the sanctions for misuse. Learning Platforms are now widely established and clear agreement by all parties about acceptable and responsible use is essential.

Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person.

They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny. Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to pupils including e-mail, home or mobile

telephone numbers, unless the need to do so is agreed with senior management and parents/carers.

E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used in accordance with the school/service's policy.

Further information can be obtained from http://www.education.gov.uk
Recommendations

(i) That this document is shared with all staff who come into contact with children and young people, that it is retained in Staff Handbooks and that it is specifically referred to when inducting new members of staff into your school/service.

(ii) (ii) That appropriate links are made to this document with your school/services Acceptable Use Policy

(iii) (iii) That employees are encouraged to consider any guidance issued by their professional association/trade union concerning the use of social networking sites

(iv) That employees are informed that disciplinary action may be taken in relation to those members of staff who choose not to follow the Specific Guidance outlined above.

This means that schools/services should:

- have in place an Acceptable Use policy (AUP) - continually self-review e.safety policies in the light of new and emerging technologies

This means that adults should: - ensure that personal social networking sites are set at private and pupils are never listed as approved contacts
- never use or access social networking sites of pupils.

- not give their personal contact details to pupils, including their mobile telephone number

- only use equipment e.g. mobile phones, provided by school/service to communicate with children, making sure that parents have given permission for this form of communication to be used

- only make contact with children for professional reasons and in accordance with any school/service policy

- recognise that text messaging should only be used as part of an agreed protocol and when other forms of communication are not possible not use internet or web-based communication channels to send personal messages to a child/young person.

Pupils' use of social media

If school staff are aware that pupils are using social media or technology inappropriately, they inform parents and pupils of the legal requirements of social media websites eg the age restrictions, and discourage their use. Parents will be informed of the age requirements.

Sexting

(Taken from document - Sexting in Schools and Colleges – Responding to Incidents and Safeguarding Young People from UK Council for Child Internet Safety.)

Response from staff:
If staff become aware of a sexting incident, they must report it to the DSL without delay.
They must not view, copy, share or delete the images as this is a criminal offence.

When an incident involving youth produced sexual imagery comes to a school or college's attention:

- The incident should be referred to the DSL as soon as possible
- The DSL should hold an initial review meeting with appropriate school staff
- There should be subsequent interviews with the young people involved (if appropriate)
- Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm
- At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately.

The circumstances of incidents can vary widely. If at the initial review stage, a decision has been made not to refer to police and/or children's social care, the DSL should conduct a further review (including an interview with the young people involved) to establish the facts and assess the risks.
When assessing the risks, the following should be considered:

- Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
- Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
- Are there any adults involved in the sharing of imagery?
- What is the impact on the pupils involved?
- Do the pupils involved have additional vulnerabilities?
- Does the young person understand consent?
- Has the young person taken part in this kind of activity before?

Part Four - Guidance on Safer Working Practice 2022

The following information has been taken from The Department for Education document 'Guidance for Safer Working Practices for Adults Working with Children and Young people in Educational Settings (2019 and 2020), and forms part of policy at Reedley:

24. Photography, videos and other images / media
Many educational activities involve recording images. These may be undertaken for displays, publicity, to celebrate achievement and to provide records of evidence of the activity.
Under no circumstances should staff be expected or allowed to use their personal equipment to take images of pupils at or on behalf of the school or setting.
All settings should have arrangements with regard to the taking and use of images, which is linked to their safeguarding and child protection policy.
This should cover the wide range of devices which can be used for taking/recording images e.g. cameras, mobile-phones, smart phones, tablets, web-cams etc. and arrangements for the use of these by both staff, parents and visitors.

Whilst images are regularly used for very positive purposes, adults need to be aware of the potential for these to be taken and/or misused or manipulated for pornographic or 'grooming' purposes. Particular regard needs to be given when images are taken of young or vulnerable children who may be unable to question why or how the activities are taking place.
Pupils who have been previously abused in a manner that involved images may feel particularly threatened by the use of photography, filming etc.
Staff should remain sensitive to any pupil who appears uncomfortable and should recognise the potential for misinterpretation. Making and using images of pupils will require the age appropriate consent of the individual concerned and their parents/carers.
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 setting have access.
For the protection of children, it is recommended that this means that staff should:
▪ adhere to their establishment's policy
▪ only publish images of pupils where they and their parent/carer have given explicit written consent to do so
• only take images where the pupil is happy for them to do so
▪ only retain images when there is a clear and agreed purpose for doing so
▪ store images in an appropriate secure place in the school or setting
▪ ensure that a senior member of staff is aware that the photography/image equipment is being used and for what purpose
▪ be able to justify images of pupils in their possession
▪ avoid making images in one to one situations

This means that adults should not:
▪ take images of pupils for their personal use
▪ display or distribute images of pupils unless they are sure that they have parental consent to do so (and, where appropriate, consent from the child)
▪ take images of children using personal equipment
▪ take images of children in a state of undress or semi-undress
▪ take images of a child's injury, bruising or similar (e.g. following a disclosure of abuse) even if requested by children's social care
▪ make audio recordings of a child's disclosure
▪ take images of children which could be considered as indecent or sexual when using images for publicity purposes that the following guidance should be followed:
• if the image is used, avoid naming the child, (or, as a minimum, use first names rather than surnames)
• if the child is named, avoid using their image
• schools and settings should establish whether the image will be retained for further use, where and for how long
• images should be securely stored and used only by those authorised to do so.

25. Use of technology for online / virtual teaching
All settings should review their online safety and acceptable use policies and amend these if necessary, ensuring that all staff involved in virtual teaching or the use of technology to contact pupils are briefed on best practice and any temporary changes to policy / procedures.
When selecting a platform for online / virtual teaching, settings should satisfy themselves that the provider has an appropriate level of security.
Wherever possible, staff should use school devices and contact pupils only via the pupil school email address / log in.
This ensures that the setting's filtering and monitoring software is enabled. In deciding whether to provide virtual or online learning for pupils, senior leaders should take into account issues such as accessibility within the family home, the mental health and wellbeing of children, including screen time, the potential for inappropriate behaviour by staff or pupils, staff access to the technology required, etc.
Virtual lessons should be timetabled and senior staff and DSL should be able to drop in to any virtual lesson at any time – the online version of entering a classroom.
Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents.
The following points should be considered:-

▪ think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be nondescript
▪ staff and pupils should be in living / communal areas – no bedrooms
▪ staff and pupils should be appropriately dressed
▪ filters at a child's home may be set at a threshold which is different to the school
▪ resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content
It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary.

Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / pupil consent is needed and retention / storage.

If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately. Staff, parent and pupil AUPs should clearly state the standards of conduct required.

If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with a senior member of staff and, if there is no alternative, always use 'caller withheld' to ensure the pupil / parent is not able to identify the staff member's personal contact details.

26. Exposure to inappropriate images
Staff should take extreme care to ensure that children and young people are not exposed, through any medium, to inappropriate or indecent images.
There are no circumstances that will justify adults: making, downloading, possessing or distributing indecent images or pseudo-images of children (child abuse images).

Accessing these images, whether using the setting's or personal equipment, on or off the premises, or making, storing or disseminating such material is illegal.

If indecent images of children are discovered at the establishment or on the school or setting's equipment an immediate referral should be made to the Designated Officer (DO) and the police contacted if relevant.

The images/equipment should be secured and there should be no attempt to view or delete the images as this could jeopardise necessary criminal action. If the images are of children known to the school, a referral should also be made to children's social care in line with local arrangements.

Under no circumstances should any adult use school or setting equipment to access pornography. Personal equipment containing pornography or links to it should never be brought into or used in the workplace.
This will raise serious concerns about the suitability of the adult to continue working with children and young people. Staff should keep their passwords confidential and not allow unauthorised access to equipment.
In the event of any indecent images of children or unsuitable material being discovered on a device the equipment should not be tampered with in any way. It should be secured and isolated from the network, and the DO contacted without delay. Adults should not attempt to investigate the matter or evaluate the material themselves as this may lead to a contamination of evidence and a possibility that they will be at risk of prosecution themselves.

Policy author: Sarah Bell Date: 01.09.19 Reviewed 01.09.20 Reviewed 01 09 21
Reviewed 01 09 24
To be reviewed 01.09.25