ROSSETT ACRE PRIMARY SCHOOL

E-Safety and ICT Acceptable Use Policy including Social Media

Members of staff responsible:	**Perveen Aslam**
Date of Policy:	**March 2021 reviewed February 2025**
Review Date:	**February 2027**

E-Safety

CONTENTS **Page(s)**

1. Rationale

The use of 'Information and Communication Technologies' (ICT) has great benefits for the development of pupils' learning and the administration and governance of a school. With these advantages, however, come risks, including:

1.1 cyber-bullying

1.2 identity theft (including phishing)

1.3 spam

1.4 viruses

1.5 child sexual exploitation

It is the aim of this policy to minimise these risks for pupils, staff and others involved within the daily activities of the school.

This policy, supported by the school's Acceptable Use Policy (Appendix 1) for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to mandatory school policies: child protection, health and safety, home–school agreements, behaviour policy and anti-bullying policy.

2. 'Un-Safe' Use of ICT

This policy is concerned with significantly unsafe use of ICT, not minor infringements. Just as safe use of ICT is commonly known as E-Safety, unsafe use of ICT is an E-Safety incident. An E-Safety incident:

2.1 uses some form of technology

2.2 causes or could have caused significant offence, harm or distress

2.3 may or may not be deliberate

2.4 may not have occurred within school or on school equipment.

Examples of E-Safety incidents (not exclusive) include:

2.5 a pupil or member of staff viewing unsuitable material on a school device

2.6 a pupil bullying a fellow pupil with text messages

2.7 a pupil bullying a fellow pupil using instant messaging services

2.8 a pupil or parent placing distressing posts about a member of the school community on social networking sites

2.9 a pupil publishing their own personal details on the internet

2.10 a pupil publishing revealing images of her or himself on a social networking site

2.11 a member of staff suspecting a pupil of being groomed through their use of internet chat services

3. Staff Responsibilities

3.1. It is the role of the Computing Subject Leader to:

3.1(a) keep abreast of current issues and guidance through organisations such as North Yorkshire LA, CEOP (Child Exploitation and Online Protection) and Childnet

3.1(b) support staff in handling incidents

3.1(c) support the education of pupils and staff in the safe use of ICT

3.2 It is the role of Red Kite Trust to: maintain services in support of the safe use of ICT. Typically to include: 3.2(a) internet and email filtering and logging

3.2(b) network access logging

3.2(c) appropriate level of network security against malicious use

3.3 Other staff:

3.3(a) are aware of what is safe use of ICT

3.3(b) model safe use of ICT, including social media, within the school community and beyond

3.3(c) are alert to unsafe use of ICT - by pupils & staff, within school and beyond

3.3(d) manage & report incidents as appropriate

3.3(e) educate pupils where required by the curriculum

4. Pupil Responsibilities

4.1 Must adhere to the Acceptable Use Policy and the Home-School Agreement

4.2 Will use the internet appropriately in school and not search for inappropriate content.

4.3 Must report incidents as they occur through the most appropriate member of staff; e.g. class teacher, Computing Subject Leader or SLT member.

5. Parent Responsibilities

5.1 To understand the Acceptable Use Policy and Home-School Agreement, and encourage their child to use ICT safely.

5.2 When attending school events and performances, any digital images taken by parents / carers are not to be published on any social media networks.
When accompanying children on school visits, parents / carers are not permitted to take images on any devices other than those issued by school for this intention.

6. Education in Safe Use of ICT

6.1 Staff

6.1(a) In addition to the annual training in Child Protection, all staff will be trained in the safe use of ICT both for themselves and for pupils they supervise; the training will be held annually via a staff meeting lead by the computing subject leader, and will be kept up-dated.
The training will raise awareness of their individual responsibilities for the safeguarding of children within the context of E-Safety and will cover what to do in the event of misuse of technology by any member of the school community.

6.1(b) All new staff will need to read the E-Safety Policy, which includes information on the school's acceptable use policy, as part of their induction - making a signed declaration this has been completed.

6.2 Pupils

6.2(a) The school will provide opportunities through the Computing Programme of Study, PSHCEe lessons, Assemblies and initiatives such as Safer Internet Day, as well as in other curriculum areas as appropriate.

6.2(b) Through the Computing Programme of Study, pupils will be taught about copyright, respecting other people's information, images, and related topics.

6.2(c) Pupils will be made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying.

6.2(d) Pupils will be taught the dangers of releasing personal information through the use of social networking platforms and instant messaging / chat facilities.

6.2(e) Pupils will also be made aware of where to seek advice or help if they experience problems when using the internet and related technologies: i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

7. Managing Technology

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education and social interaction, as well as a potential risk to young and vulnerable people.

7.1 Infrastructure

Schools ICT will monitor access and use of the school network including internet services. Email and internet activity can be monitored and explored further if required. Rossett Acre Primary School will be aware of its responsibility when monitoring staff and pupil communication under current legislation and take into account:

7.1(a) Data Protection Act 1998,

7.1(b) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000,

7.1(c) Regulation of Investigatory Powers Act 2000,

7.1(d) Human Rights Act 1998

7.1(e) Also, with regard to cyber bullying or other harmful communication:

- Protection from Harassment Act 1997
- Criminal Justice & Public Order Act 1994
- Malicious Communications Act 1988
- Communications Act 2003
- Defamation Act 2013

The school also reserves the right to inspect any computing device authorised for school activity use.

7.2 Managing the Internet
Access to the internet will be monitored by Schools ICT.

Staff will make every effort to preview sites and applications before recommending them to pupils; it is recognised that internet sites and applications are beyond the control of Rossett Acre Primary School.

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

Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended audience. Users must not reveal personal information/images about members of the school community (including names) acquired through school life on any social networking site or blog without seeking the subject's permission. Information published on the internet prior to the adoption of this policy may remain where not causing an issue; however, staff should declare any material in the public domain (to the Designated Safeguarding Lead or the Designated Safeguarding Persons) which will be inspected for suitability.

The school strongly advises that staff do not accept friend requests on personal accounts from pupils, past or present, or from parents at the school.

8. <u>Communication</u>

Pupils, Parents, Staff and Governors are made aware of the School's E-Safety Policy through a variety of means:

8.1 The E-Safety policy will be introduced to the pupils at the start of each school year and displayed on the school website.

8.2 E-Safety messages will be embedded across the curriculum whenever the internet and/or related technologies are used including Assemblies.

8.3 E-Safety posters will be prominently displayed around school.

8.4 E-Safety updates will be displayed via the following methods:

8.4(a) schoolwebsite

8.4(b) school newsletter

9. Specific E-Safety Issues

Further advice is available at: http://www.itgovernance.co.uk/

9.1 Digital images & video

Digital images are easy to capture, reproduce and publish and, therefore, misuse. It is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils. Staff should only take photographs or videos of pupils with the express permission of pupil and parent. This is normally obtained from parents on entry to the school and a list of the pupils whose parents have objected to this is kept by the School Office. It is essential that school equipment is used for this, but in any case, images must be transferred within a reasonable time scale and solely to the school's network or hosted services controlled by the school and deleted from the original device. Staff must not share or store images of pupils on their own Personal Mobile Device (PMD) or personal social media networks.

Pupils must be advised when using personal digital equipment, especially during school visits, that images and video should only be taken and shared with the subjects' consent.

Permission to use images and video of all staff who work at the school is sought on induction and a copy is to be stored in the relevant personnel file.

9.2 Publishing Pupil's Images and Work

On a pupil's entry to the school, all Parents/carers are asked to give permission to use their pupil's work / photos in the following ways:

9.2(a) on the school web site

9.2(b) in the school prospectus and other printed publications that the school may produce for promotional purposes

9.2(c) recorded/ transmitted on a video or webcam

9.2(d) in display material that may be used in the school's communal areas

9.2(e) in display material that may be used in external areas, ie exhibition promoting the school

9.2(f) general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/carers may withdraw permission, in writing, at any time. Consent has to be given by all interested parties in order for it to be deemed valid. Pupils' full names will not be published alongside their image by the school and vice versa. E-mail and postal addresses of pupils will not be published. Often, the press wishes to publish full names for members of teams. In these cases, the member of staff supervising will ensure that appropriate permission is sought. Before posting pupil work on the Internet, the member of staff responsible must check that permission has been given for work to be displayed.

9.3 Personal Mobile Devices (PMDs) including iPADs, phones and other PMDs provided by school

9.4(a) The school allows staff to bring in PMDs for their personal use. Under no circumstances does the school allow a member of staff to use an identifiable PMD/personal email account to contact a pupil or parent.

9.4 (b) Staff are advised not to contact a parent/carer using their PMD but there may be circumstances concerning a duty of care to pupils which override this.

9.4(c) Pupils are not allowed to bring mobile phones to school, unless they are in Upper Key Stage 2 and there is a legitimate reason e.g. they are walking home alone – these devices should be handed in to the teacher at the beginning of each day.

9.4(d) The school is not responsible for the loss, damage or theft of any personal PMD.

9.4(e) The sending of inappropriate (as determined by any involved party) text messages between any member of the school community is not allowed.

9.4(f) Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

9.4(g) Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

9.4(h) Where the school provides mobile technologies such as iPADs, phones, laptops for offsite visits and trips, these devices must be used.

9.4(i) Where members of staff use PMDs to access school services such as email or the intranet, they should not download personal information such as lists of pupil names to their device.

9.4(j) Where members of staff use PMDs to access school services, password protection is mandatory in case of theft or loss. Any staff losing a PMD which is configured for school data services must report the loss to the school office as soon as practical.

9.5(k) PMDs for personal use should not be used in the vicinity of children.

10. Further Guidance

Websites offering help and advice:

- http://www.anti-bullyingalliance.org.uk
- http://www.itgovernance.co.uk/
- http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml
- http://www.thinkuknow.co.uk
- http://www.leedslearning.net/documents/E-

Safety/Chat%20Room%20Dangers%20and%20computer%20safety.doc

- http://www.ceop.gov.uk/
- http://www.getsafeonline.org/
- http://www.parentscentre.gov.uk/flash/safety/main.swf
- http://www.kidsmart.org.uk/
- http://www.microsoft.com/athome/security/children/default.mspx
- http://www.parentscentre.gov.uk/
- http://schools.becta.org.uk/index.php?section=is
- http://publications.becta.org.uk/display.cfm?resID=32424&page=1835
- http://www.digizen.co.uk/
- http://www.portal.northerngrid.org/ngflportal/custom/resources_ftp/client_ftp/E-Safety_audit_tool/E-Safety_audit_tool.html
- http://www.nextgenerationlearning.org.uk/safeguarding

11. Procedures for Monitoring and Reporting Incidents

The Head Teacher:

The Head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The DSL:

Details of the school's DSL and DDSL are set out in the Child Protection and Safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Carrying out half termly Filtering and Monitoring checks;
- Working with staff to address any online safety issues or incidents;
- Managing all online safety issues and incidents in line with the school's Child Protection and Safeguarding policy;
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's Behaviour and Anti Bullying policies;
- Providing regular reports on online safety to the LGB.

The Computing Leader:

The computer leader supports the DSL and takes responsibility for:

- Supporting the Investigation of any reported incidents;
- Carrying out termly full monitoring of school devices;
- Carrying out half termly 'spot checks' on school devices;
- Providing advice to staff regarding online safety;
- Updating and delivering staff training on online safety and recording the training;
- Liaising with other agencies and/or external services if necessary;

11.1 Pupil E-Safety incidents:

Many incidents of misbehaviour involving ICT do not lead to actual or potential significant offence, harm or distress. These should be dealt with by our normal discipline procedures. Where the member of staff involved believes the event to be an E-Safety incident, they will follow this procedure:

11.1(a) Log the incident on CPOMS alerting the Designated Safeguarding Lead and the Computing Subject Leader.

11.1(b) The Designated Safeguarding Lead Computing and Subject Leader to investigate and decide whether further action should be taken.

11.1(c) Further action may include sanctions or education and may involve parents. In extreme cases, it may be necessary to involve outside agencies such as the Police or the local authority.

11.2 Staff E-Safety incidents

If a member of staff suspects another member of staff has breached this policy, they should report their concerns to the Designated Safeguarding Lead or the SLT. This will be investigated to see if further action is needed. Any internal disciplinary action taken will conform to the Staff Discipline policy. If a criminal offence has been committed, the details will be passed on to the appropriate authorities.

12. Staff to acknowledge reading the E-Safety Acceptable use policy via an online form.

Appendix 1

ICT Acceptable Use Policy

Scope of this policy

Who: whoever uses ICT at Rossett Acre Primary School (pupils, parents, visitors, governors and staff)

What: any ICT related item, from cameras, iPADs and computers to use of web applications including blogging.

Why: to keep our use of technology safe for all of us to enable help with learning

Where: both in school and out of school this policy applies to whenever anyone uses ICT-related equipment or services

Allowed: ICT is provided by Rossett Acre Primary School for educational purposes only. You are responsible for your use of ICT as you are for any other personal behaviour. This includes your password, and you must keep this private. You should respect the work of others and not copy published material without permission. Use of internet resources must be appropriate for educational purposes.

Unacceptable:

Hacking: accessing unauthorised devices and areas of the network, even if you do this without meaning to cause a problem.

Viruses: intentional distribution of viruses causes serious damage to network resources and is illegal.

Offensive material: the creation, publication, sharing (including by email) or viewing of anything considered to be offensive or abusive, to either an individual or group will not be tolerated.

Disruptive actions: unauthorised social networking, spam email, wasting of staff time by interfering with equipment, wasting network resources through unauthorised streaming video or unauthorised downloading and storing of large files, causing distress by cyberbullying.

Consequences: Access to ICT services is provided to users who agree to act in a considerate and responsible manner. Loss of this privilege is a natural consequence of abuse.
Failure to follow this Acceptable Use Policy will result in the current school sanctions to be applied at an appropriate level, as decided by class teachers, the Senior Leadership Team, or the Governing Body.

By using the ICT provision at Rossett Acre Primary School you have agreed you understand and will abide with this Acceptable Use Policy.

Name ____________________________

Signature ____________________________

NB Staff are bound by this as a condition of their employment