Rockcliffe CE School

Online Safety Policy

2021 - 2022

This policy should be reviewed in July 2022

Covid-19 response on loaned items included.

1. Aims of the Policy

This Online Safety Policy aims to ensure that all pupils and their parents/carers will:

- behave at all times within the terms of current legislation and the expectations of the school community;
- only use school IT resources to develop the pupils' skills and knowledge in the context of the wider school curriculum;
- make careful and considerate use of the schools IT resources, report faults and work in a way that minimises the risk of introducing computer viruses to the system;
- protect everyone in school from the harmful or inappropriate material accessible via the Internet or transportable on computer media;
- use email and similar systems appropriately;
- recognise their responsibility to maintain the privacy of individuals;
- know and abide by the schools E-Safety Policy as it applies to them.

The role of the Governors is to:

- ensure that the school follows all current online safety advice to keep the children and staff safe;
- approve the Online Safety Policy and procedures and review its effectiveness.
- support the school in encouraging parents and the wider community to become engaged in online safety activities;

The Head teacher will:

- take overall responsibility for data and data security;
- ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements;
- be aware of the procedures to be followed in the event of a serious online safety incident or an allegation being made against a member of staff or volunteer

Teachers must:

- ensure that online safety issues are embedded in all aspects of the curriculum and other school activities, particular within RSHE;
- monitor, supervise and guide pupils carefully when engaged in ICT activity in lessons, extra-curricular and extended school activities;
- ensure that pupils are fully aware of research skills and are made aware of legal issues relating to electronic content such as copyright laws.
- ensure that during lessons where internet use is pre-planned pupils are guided to sites checked as suitable for their use and that processes are known and used when dealing with any unsuitable material that is found in internet searches.

2. Who is covered by the policy?

This policy relates to all children and adults who use any IT equipment in school – this may include PCs, laptops, notebooks, tablets, smart phones, memory sticks or any other new technology with similar applications. It also relates to children and adults working off-site, for example at home, but accessing the school website, learning platform or other applications recommended by school as part of school work.

3. Legal Issues

All of the school's software is legally licensed and catalogued. No software can be added to machines unless permission has been given by the school's IT subject leader.

No material is to be shared (either via e-mail or via the school's website) until it has been checked by the school's IT subject leader. This will ensure that no copyright laws are broken.

4. Access to the network

Access to the curriculum Wi-Fi network is password controlled.

Access to the administrative network is limited to the administrator, Assistant Head teacher and Head teacher, and is password controlled.

5. Website, Internet and Email Access

Published content and the school web site

The school will only publish its own address, contact details on the school website. Pupils' personal information will never be published on the school's website.

Generic permission from parents or carers will be checked before photographs of pupils will be published on the school website.

The school's headteacher will take overall editorial responsibility and ensure that content is both accurate and appropriate at all times.

Safe surfing of the Internet

At Rockcliffe CE School we aim to keep our children safe when using the Internet. The Internet Service Provider (ISP) used by the school is that recommended by Cumbria County Council. This ISP provides a filtering service which eliminates unsuitable material from the Internet. Pupils should be made aware of this and encouraged to instantly report any unsuitable material that they may encounter on the Internet. If pupils discover an unsuitable site, they must report the site to the class teacher, who in turn will notify the IT subject leader. Pupils should be told NOT to turn the actual computer off.

Staff must report unsuitable material encountered on the Internet immediately to either the IT Co-ordinator/Headteacher. The ISP will then be contacted to eliminate the material. Parents will be informed that unsuitable material has been accessed.

Social networking sites

The school's Internet Service Provider has blocked all social networking sites so children are unable to access them at school (see above).

In addition, we teach our children to never to give out personal details of any kind which may identify them or their location.

E-mail

Pupils may only use approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Virus Protection

The school has an annual subscription to Sophos. This software ensures that all networked machines are kept up to date against viruses. In addition, all machines' operating systems and browsers are kept up to date, to minimise the possibility of a virus attack.

Pupils should not bring in from home any IT device (see 2 above) nor connect them to IT equipment in school without permission from the IT co-ordinator/Headteacher.

Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left;
- Prompt action on disabling accounts will prevent unauthorised access.

6. Privacy

The school will only use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school or CCC. For other members of the community, the school will advise in advance if it is necessary to pass the information on to anyone else other than the school and CCC

The school will hold personal information on its systems for as long as someone remains a member of the school community and remove it in the event of leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Cumbria County Council and as defined by the Data Protection Act 1998.

Anyone has the right to view the personal information that the school holds about them and to have any inaccuracies corrected.

7. Use of digital images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, students/pupils and parents/carers need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

7.1 Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
7.2 Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
7.3 Students/pupils must not take, use, share, publish or distribute images of others without their permission.
7.4 Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images. Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

8. Assessing Risks

Rockcliffe CE School will:

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- *The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Cumbria Police.*
- *Methods to identify, assess and minimise risks will be reviewed regularly.*

8.1 Unsuitable/Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

9. Mobile Phones

The use of mobile phones and other personal devices by pupils and staff in school will be decided by the school and covered in the school Acceptable Use Agreement.
The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/Behaviour Policy.
The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable materials, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.
School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour Policy or bullying procedures.

10. Loaned resources

We have identified a pool of machines that can be loaned out to families deemed disadvantaged in the case of a lockdown.
Any loaned resources will be wiped and a new install of software added on the return of the item to school. Any returned items cannot be accessed by any staff member or connected to the school network until a wipe has taken place.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					✓	
On-line gaming (educational)						

On-line gaming (non-educational)					
On-line gambling					
On-line shopping/commerce					
File sharing					
Use of social networking sites					
Use of video broadcasting e.g. Youtube					

8.2 Assessing Risks

The risks that can be posed to young people and adults when online have been identified by the EUKids online project, which was later referenced in paragraph 1.3 of Dr Tanya Byron in "Safer Children in a Digital World" (2008).

	Commercial	Aggressive	Sexual	Values
Content (Child as recipient)	Adverts Spam Sponsorship Personal Info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias, Racist or Misleading info or advice
Contact (Child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers, Being groomed	Self-harm, Unwelcome persuasions
Conduct (Child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading information/advice

1.1 Responding to Incidents of Concern

If any apparent or actual misuse appears to involve illegal activity i.e.

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

school should refer to the Flow Chart found at Appendix H.

- *All members of the school community will be informed about the procedure for reporting E-Safety concerns (such as breaches of filtering, cyber-bullying, illegal content etc.).*
- *The Designated Safeguarding Lead will be informed of any E-Safety incidents involving Child Protection concerns, which will then be escalated appropriately – See Child Protection Policy for dealing with concerns.*
- *The school will manage E-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.*
- *The school will inform parents/carers of any incidents of concerns as and when required.*
- *After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.*
- *Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Children's Services and escalate the concern to the Police.*
- *Any racist incidents will be reported to Children's Services. Racist Incident Monitoring forms should be completed electronically through the* ***School Portal****. This allows for individual incidents to be reported as and when they happen and will also generate a termly report for schools to agree to and return.*
- *If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Local Authority Designated Officer (LADO) – see Child Protection Policy.*

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. More than one member of staff should be involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Students/Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher/tutor	Refer to Head of Department/Head of Year/other	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		✓	✓	✓					
Unauthorised use of non-educational sites during lessons									
Unauthorised use of mobile phone / digital camera / other handheld device									
Unauthorised use of social networking / instant messaging / personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school network by sharing username and passwords									
Attempting to access or accessing the school network, using another student's/pupil's account									
Attempting to access or accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Head teacher	Refer to LA/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email								
Unauthorised downloading or uploading of files								
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account								
Careless use of personal data e.g. holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature								
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school								
Using proxy sites or other means to subvert the school's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material								
Breaching copyright or licensing regulations								
Continued infringements of the above, following previous warnings or sanctions								

Handling online safety Complaints

- **Complaints about Internet misuse will be dealt with under the School's complaints procedure.**
- **Any complaint about staff misuse will be referred to the head teacher.**
- **All e–safety complaints and incidents will be recorded by the school on CPOMS, including any actions taken.**
- *Pupils and parents will be informed of the complaints procedure.*
- *Parents and pupils will need to work in partnership with the school to resolve issues.*
- *All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.*
- *Discussions will be held with the local Police and/or Children's Services to establish procedures for handling potentially illegal issues.*
- *Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.*
- *All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community or which may bring the school into disrepute.*

Rules for Responsible Use of IT

The school has installed computers with Internet access to help your learning. These rules will keep you safe

- Always ask permission from a member of staff before using the Internet.
- Do not access other people's files without permission.
- Only use the computers for school work.
- Do not bring in memory sticks from outside school unless you have been given permission.
- Only send e-mail to people that your teacher has approved.
- Only send polite messages.
- Never give out any addresses, telephone numbers or
- arrange to meet someone unless your parent or teacher know and have given you permission.
- Do not give names of friends or family members to anybody on the Internet
- Do not go into any 'chat rooms' (These should already be blocked)
- If you see any unpleasant material, or have unsuitable messages sent to you, tell a member of staff immediately (DO NOT turn off the actual computer itself).

The school may check your computer files and may monitor the Internet sites that you visit.