



# E-Safety Policy

	<b>Name</b>	<b>Date</b>
Reviewed	Danielle Wood	September 2018
Next Review		November 2019

## **INTRODUCTION**

E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of E-Safety at all times, to know the required procedures and to act on them.

This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

The Headteacher or, in their absence, the authorised member of staff for E-Safety has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

This policy complements and supports other relevant school and Local Authority policies.

The purpose of internet use in school is to help raise educational standards, promote pupil achievement, support the professional work of staff as well as enhance the school's management information and business administration systems.

The internet is an essential element in 21<sup>st</sup> Century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience.

A risk assessment will be carried out before children and young people are allowed to use new technology in schools and associated settings.

## **ETHOS**

It is the duty of the school to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the Every Child Matters agenda apply equally to the 'virtual' or digital world. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.

All staff have a responsibility to support E-Safety practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach E-Safety protocols.

E-Safety is a partnership concern and is not limited to school premises, school equipment or the school day.

Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with the school's Behaviour and Relationships Policy.

Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Children Policy.

## **ROLES AND RESPONSIBILITIES**

The Headteacher will ensure that:

- All staff should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A Designated Senior Member of Staff for E-Learning/Safety is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.
- All temporary staff and volunteers are made aware of the school's E-Safety Policy and arrangements.
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

The Governing Body of the school will ensure that:

- There is a senior member of the school's leadership team who is designated to take the lead on E-Learning/Safety within the school.
- Procedures are in place for dealing with breaches of E-Safety and security and are in line with Local Authority procedures.
- All staff and volunteers have access to appropriate ICT training.

The Designated Senior Member of Staff for E-Learning/Safety will:

- Act as the first point of contact with regards to breaches in E-Safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.

Raglan Primary School and Nursery  
Part of Connect Schools Academy Trust

- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on E-Safety.
- Ensure that all staff and volunteers have received a copy of the school's Acceptable Use of ICT Resources document.
- Ensure that all staff and volunteers understand and aware of the school's Social Media and Networking Policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Discuss security strategies with the Local Authority particularly where a wide area network is planned.
- Regularly check files on the school's network.

## **TEACHING and LEARNING**

### **Benefits of internet use for education**

- The internet is a part of the statutory curriculum and a necessary tool for staff and children and young people and benefits education by allowing access to world - wide educational resources including art galleries and museums as well as enabling access to specialists in many fields for pupils and staff.
- Access to the internet supports educational and cultural exchanges between students world-wide and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.
- The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority and DFE.
- The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives.
- The internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.
- Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the

Raglan Primary School and Nursery  
Part of Connect Schools Academy Trust

curriculum requirements and age of the children and young people.

- Children and young people will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Children and young people will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Children and young people will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

### **Managing Internet Access**

- Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children and young people.
- Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.
- Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Co-ordinator.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

### **Managing E-Mail**

- Personal e-mail or messaging between staff and pupils should not take place.

Raglan Primary School and Nursery  
Part of Connect Schools Academy Trust

- Staff must use the school e-mail address if they need to communicate with pupils about their school work e.g. study leave, course work etc.
- Pupils and staff may only use approved e-mail accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive e-mail. Whole-class or group e-mail addresses should be used at KS1 and below.
- Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and will be restricted.
- E-mail should be authorised before sending to an external organisation just as a letter written on school headed note-paper would be.  
The forwarding of chain letters is not permitted.
- Incoming e-mail should be monitored and attachments should not be opened unless the author is known.

### **Managing Website Content**

- Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.
- Photographs of pupils will not be used without the written consent of the pupil's parents/carers.
- The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or pupil's home information will not be published.
- The Headteacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.
- The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.
- Use of site photographs will be carefully selected so that any pupils cannot be identified or their image misused.

Raglan Primary School and Nursery  
Part of Connect Schools Academy Trust

- The names of pupils will not be used on the website, particularly in association with any photographs.
- Work will only be used on the website with the permission of the pupil and their parents/carers.
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.
- Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

### **Social Networking and Chat Rooms**

- Pupils will not access social networking sites eg 'My Space', 'Facebook' or 'Twitter'.
- Pupils should not post messages on social networking sites or other sharing sites such as You Tube, that are inappropriate, either about the staff, pupils, parents or about the school community.
- Pupils will be taught the importance of personal safety when using social networking sites and chat rooms.
- Pupils will not be allowed to access public or unregulated chat rooms.
- Pupils will only be allowed to use regulated educational chat environments and use will be supervised.
- Pupils will be advised to use nick names and avatars when using social networking sites.
- Staff will not exchange social networking addresses or use social networking sites to communicate with pupils.
- Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil is necessary, the agreement of a senior manager should always be sought first and language should always be appropriate and professional.

### **Inappropriate Material**

- Any inappropriate websites or material found by pupils or school personnel will be reported to the E-Safety Coordinator who in turn will report to the Internet Service Provider.

### **Mobile Phones**

- **Mobile phones will not be used in school.**
- Use of cameras in their mobile phones are not to be used in school
- Staff will be issued with a school mobile phone where contact with pupils is necessary or where mobile phones are used to photograph school activities involving pupils.

### **Filtering**

- The school will work in partnership with parents/carers, the Local Authority, the DfE and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.
- If staff or pupils discover unsuitable sites, the URL (**address**) and content must be reported and the E-Safety Co-ordinators informed.
- Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation Regular checks by Senior Leadership Team will ensure that the filtering methods selected are appropriate, effective and reasonable.
- Filtering methods will be selected by the school in conjunction with the LA and will be age and curriculum appropriate.

### **Authorising Internet Access**

- All staff must read 'Staff Code of Conduct' before using any school ICT resources. The school will maintain a current record of all staff and pupils who are allowed access to the school's ICT systems.
- The school will maintain a record of pupils whose parents/carers have specifically requested that their child be denied internet or e-mail access.
- Parents/carers will be asked to sign and return the school's form stating that they have read and understood the school's 'Responsible Internet Use' document and give permission for their child to access ICT resources.
- Staff will supervise access to the internet from the school site for all pupils.

### **Photographic, Video and Audio Technology**

- When not in use all video conferencing cameras will be switched off and turned towards the wall.
- It is not appropriate to use photographic or video technology in changing rooms or toilets.
- Staff may use photographic or video technology to capture to support school trips and appropriate curriculum activities.
- Audio and video files may not be downloaded without the prior permission of the network manager.
- Pupils must have permission from a member of staff before making or answering a videoconference call or making a video or audio recording in school or on educational activities.
- Videoconferencing and webcam use will be appropriately supervised for the pupil's age.

### **Assessing Risks**

- Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.
- In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.
- Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.
- The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.

Raglan Primary School and Nursery  
Part of Connect Schools Academy Trust

- Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

### **Introducing the Policy to Pupils**

- Rules for Internet access will be posted in all rooms where computers are used.
- Responsible Internet use, covering both school and home use, will be included in the PSHE curriculum.
- Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the Internet.
- Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

### **Consulting Staff**

It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

- All staff are governed by the terms of the school's 'Staff Code of Conduct' and are provided with a copy of this.
- All new staff will be given a copy of the policy during their induction.
- Staff development in safe and responsible use of the internet will be provided as required.
- Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.
- The Senior Leadership Team will supervise members of staff who operate the monitoring procedures.

### **Maintaining ICT Security**

- Personal data sent over the network will be encrypted or otherwise secured.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mails.
- The ICT Manager will ensure that the system has the capacity to deal with increased traffic caused by Internet use.

### **Dealing with Complaints**

Raglan Primary School and Nursery  
Part of Connect Schools Academy Trust

- Staff, children and young people, parents/carers must know how and where to report incidents. Concerns related to Safeguarding issues must be dealt with through the school's Safeguarding Children Policy and Procedures.
- The school's designated person for E-Safety will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Headteacher immediately.
- Pupils and parents/carers will be informed of the complaints procedure.
- Parents/carers and pupils will work in partnership with the school staff to resolve any issues.
- As with drugs issues, there may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.
- Sanctions for misuse may include any or all of the following:
  - Interview/counselling by an appropriate member of staff
  - Informing parents/carers
  - Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system, including examination coursework.
  - Referral to the police.

### **Parents/Carers Support**

- Parents/carers will be informed of the school's Internet Policy which may be accessed on the school website and in the school brochure.
- Any issues concerning the Internet will be handled sensitively to inform parents/carers without undue alarm.
- Advice on filtering systems and appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/carers.
- Interested parents/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP).
- A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.

### **Community Use**

- School ICT resources may be increasingly used as part of the extended school agenda

Raglan Primary School and Nursery  
Part of Connect Schools Academy Trust

- Parents/carers of children and young people under 16 years of age will be required to sign the Responsible Internet Use Agreement on behalf of their child.
- Ensure that your child is not left on the computer for a sustained period of time.
- This website provides useful information:  
[www.thinkuknow.co.uk/parents](http://www.thinkuknow.co.uk/parents)

## TRAINING

We ensure all school staff have equal chances of training, career development and promotion.

Periodic training will be organised for all school personnel so that they are kept up to date with new information and guidelines concerning equal opportunities.

## MONITORING AND EFFECTIVENESS OF POLICY

The practical application of this policy will be reviewed annually or when the need arises by the coordinator, the Headteacher and the nominated Governor.

## LINKED POLICIES

- Safeguarding Children Policy
- ICT Policy
- Responsible Internet Use Agreement
- Behaviour and Relationships Policy
- Social Media and Networking Policy

## APPENDIX 1

**Annual E-Safety Audit Form:** This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for E-Safety policy. Many staff could contribute to the audit including: Designated Child Protection Coordinator, SENCO, E-Safety Coordinator, Network Manager and Headteacher.

Has the school an E-Safety Policy that complies with Kent guidance?	Yes
The policy is available for staff at:	On Sharedarea/Teaching Staff/Policies/
The policy is available for parents/carers at:	

Raglan Primary School and Nursery  
Part of Connect Schools Academy Trust

www.raglan.bromley.sch.uk	
The responsible member of the Senior Leadership Team is: Danielle Wood	
The responsible member of the Governing Body is: Chair	
The Designated Child Protection Co-ordinator is: Kath Margetts	
The E-Safety Co-ordinators are: Danielle Wood	
Has E-Safety training been provided for both pupils, parents and staff?	<b>In February 2017 training sessions were given to Parents, Staff and children in Year 5 &amp; 6</b>
Is there a clear procedure for a response to an incident of concern?	<b>Yes any concerns to be written in the E-Safety book kept in ICT suite.</b>
Have E-Safety materials from CEOP and Becta been obtained?	<b>Yes Ceop made available to parents Links on school website</b>
Do all staff sign a Code of Conduct on appointment?	<b>Yes – Introduction pack to new staff</b>
Are all pupils aware of the School's E-Safety Rules?	<b>Every computer in the school has a poster displaying safety rules.</b>
Are E-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	<b>Yes – As above</b>
Do parents/carers sign and return an agreement that their child will comply with the School E-Safety Rules?	<b>Yes – on entry to school</b>
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	<b>Yes - see E-Safety Policy on website</b>
Has an ICT security audit been initiated by SLT, possibly using external expertise?	<b>Yes</b>
Is personal data collected, stored and used according to the principles of the Data Protection Act?	<b>Yes</b>
Is Internet access provided by an approved educational Internet service provider which complies	<b>Yes</b>

Raglan Primary School and Nursery  
Part of Connect Schools Academy Trust

with DCSF requirements (e.g. KCN, Regional Broadband Consortium, NEN Network)?	
Has the school-level filtering been designed to reflect educational objectives and approved by SLT?	<b>Yes</b>

**Useful resources for teachers**

Child Exploitation and Online Protection Centre: [www.ceop.gov.uk](http://www.ceop.gov.uk)

Childnet: [www.childnet-int.org](http://www.childnet-int.org)

Cyber Café: [http://thinkuknow.co.uk/8\\_10/cybercafe/cafe/base.aspx](http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx)

Digizen [www.digizen.org](http://www.digizen.org)

Kidsmart: [www.kidsmart.org.uk](http://www.kidsmart.org.uk)

Kent Police – E-Safety:

[http://www.kent.police.uk/advice/personal/internet/young\\_people.html](http://www.kent.police.uk/advice/personal/internet/young_people.html)

Think U Know: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

UK Council for Child Internet Safety (UKCCIS):

<https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis>

**Useful resources for parents**

Family Online Safe Institute: [www.fosi.org](http://www.fosi.org)

Internet Watch Foundation: [www.iwf.org.uk](http://www.iwf.org.uk)