The Federation of Rawcliffe Bridge and Rawcliffe Primary School

ESafety Policy

Date created	January 2019	
Reviewed		
Changes		
Review date	January 2022	

1. INTRODUCTION

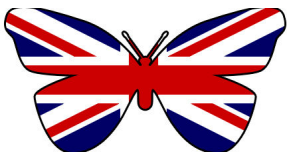
This policy has been developed to ensure that all stakeholders at Rawcliffe Bridge and Rawcliffe Primary School work to ensure safeguarding and promotes the welfare of children and young people. We aim to put effective management systems in place to maximise the education and social benefits obtained from computing use whilst minimising the risks.

This policy relates to other policies including those for computing, behaviour and for child protection.

2. TEACHING AND LEARNING

Internet Access

• The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
• Our internet provision will be filtered using the LA mediated filtering system.
• Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
• Internet use will enhance learning
• The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
• Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
• Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
• Pupils will be shown how to publish and present information to a wider audience.
• Pupils will be taught how to evaluate Internet content.
• The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
• Pupils will be taught the importance of cross-checking information before accepting its accuracy.



• Pupils will be taught how to report unpleasant Internet content.

E-mail

• When available, pupils may only use approved e-mail accounts on the school system.
• Pupils must immediately tell a teacher if they receive offensive e-mail.
• In e-mail communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
• Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
• The school should consider how e-mails from pupils to external bodies is presented and controlled.
• The forwarding of chain letters is not permitted.

3. PUBLISHED CONTENT AND THE SCHOOL WEBSITE

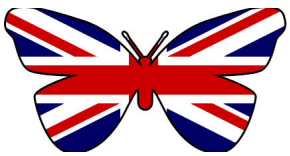
• Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
• The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
• Video or Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused.
• Pupils' names will not be used in association with video or photographs anywhere on the school Web site or other on-line space.
• Video, Pictures and work will only be shown on the website if parents/carers have signed the consent form issued at the start of each school year.
• Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

4. SOCIAL NETWORKING AND PERSONAL PUBLISHING

• Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
• Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
• Pupils will be advised to use nicknames and avatars when using social networking sites.
• Currently we do not use social networking sites as part of the curriculum.

5. MANAGING EMERGING TECHNOLOGIES

• Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
• Staff note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
• Mobile phones will not be used during lessons or formal school time. The sending of abusive or



inappropriate text messages or files by Bluetooth or any other means is forbidden.

6. PROTECTING PERSONAL DATA

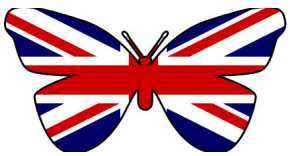
Personal data will be recorded, processed, transferred and made available according to the The Data Protection Act 2018 (DPA 2018)

- Whilst the transfer of data from home to school is inevitable, sensitive or personal data will not be taken home.
- Use of USB sticks will be avoided, but where essential, encrypted USB sticks will be used
- Logins and passwords will be kept private and where ever possible difficult to guess and certainly never written down.
- Computers will be locked when not in use.

See also the schools' 'Data Protection Policy'

7. PROCEDURES

- The School computing system's security will be reviewed regularly.
- Virus protection will be updated regularly.
- Acceptable use posters will be displayed around the school.
- The school will work in partnership with parents and the local authority to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the local authority via the computing co-ordinator and the E-Safety Coordinator informed (Reporting sheet and Protocol Appendix 1,2,3).
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- The school should audit computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.
- E-Safety training will be embedded within the computing scheme of work or the Personal Social and Health Education (PSHE) curriculum.
- E-Safety briefings and materials will regularly be made available to parents.
- Staff will always use a suitable and safe search engine when accessing the web with pupils.
- Pupils will be taught how to block someone online or report them using the CEOP button.
- Staff should be aware that internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.
- Under normal circumstances, no member of staff should engage in direct communication (in or out of

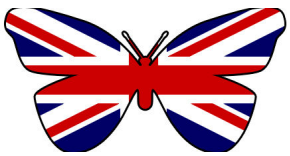


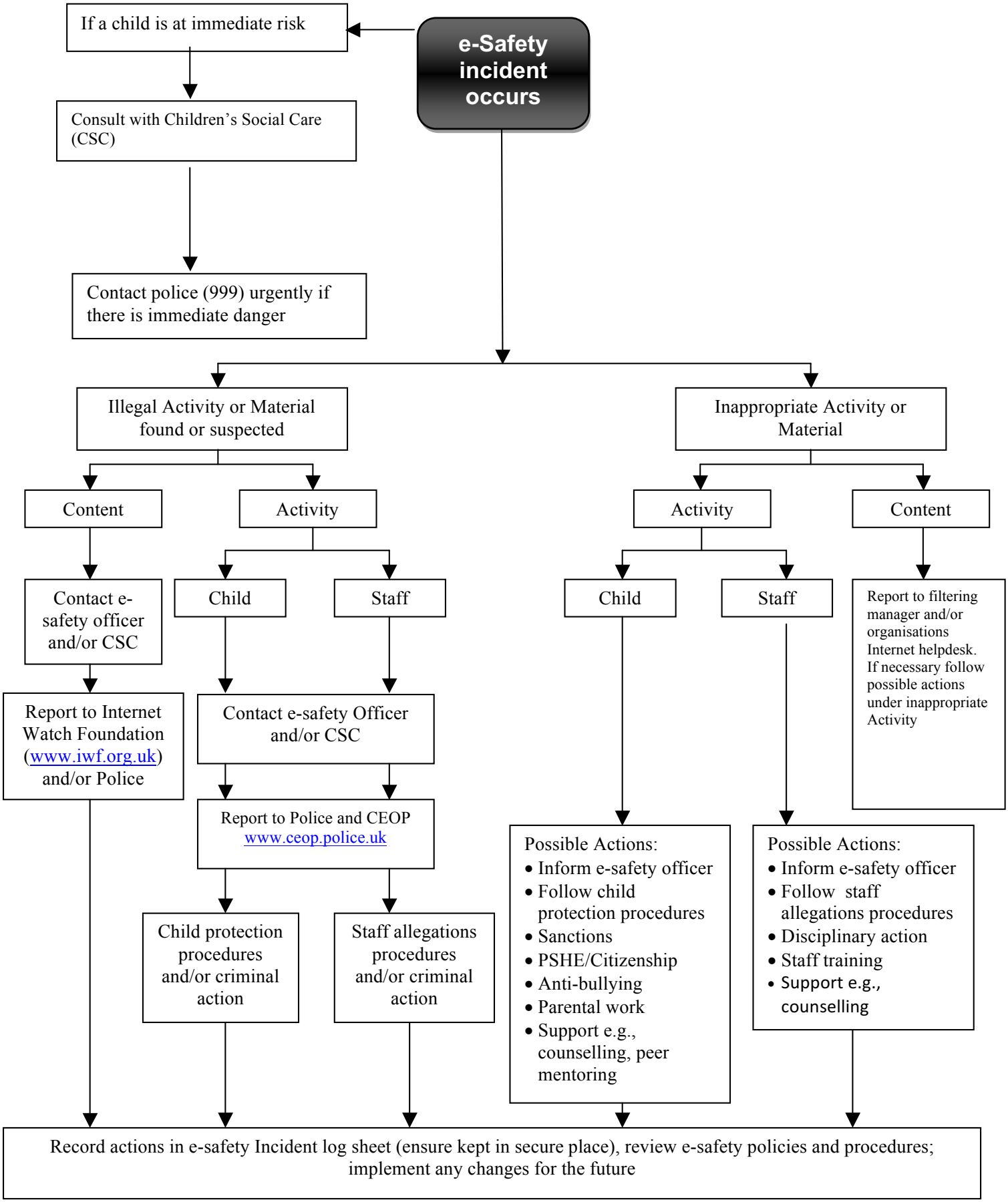
school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging or telephone. Should special circumstances arise where such communication is felt to be necessary, the agreement of a line manager should be sought first and appropriate professional language should always be used.

- Staff must not use mobile phones during teaching time or use camera phones.
- Cyber-bullying will be dealt with using the schools behaviour protocols and is seen as a serious offence.
- A planned programme of E-safety training will be made available to staff.
- All new staff will receive E-safety training as part of the induction process, ensuring they fully understand the school e-safety policy and Acceptable Use Agreements.

8. HANDLING ESAFETY COMPLAINTS

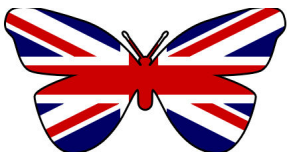
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with School child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will ask all pupils and staff to sign the relevant agreements when children are admitted.




e-Safety incident occurs
If a child is at immediate risk
Consult with Children's Social Care (CSC)
Contact police (999) urgently if there is immediate danger
Illegal Activity or Material found or suspected
Inappropriate Activity or Material
Content
Activity
Activity
Content
Contact e-safety officer and/or CSC
Child
Staff
Child
Staff
Report to filtering manager and/or organisations Internet helpdesk. If necessary follow possible actions under inappropriate Activity
Report to Internet Watch Foundation (www.iwf.org.uk) and/or Police
Contact e-safety Officer and/or CSC
Report to Police and CEOP www.ceop.police.uk
Child protection procedures and/or criminal action
Staff allegations procedures and/or criminal action
Possible Actions:
• Inform e-safety officer
• Follow child protection procedures
• Sanctions
• PSHE/Citizenship
• Anti-bullying
• Parental work
• Support e.g., counselling, peer mentoring
Possible Actions:
• Inform e-safety officer
• Follow staff allegations procedures
• Disciplinary action
• Staff training
• Support e.g., counselling
Record actions in e-safety Incident log sheet (ensure kept in secure place), review e-safety policies and procedures; implement any changes for the future

e-Incident Log Sheet 1 – "member of staff identifying incident" – front cover

To be completed by the member of staff identifying the incident					
Date of identification:		Date of incident (if different):			
Time of identification:		Time of incident (if different):			
Duration of incident:		Do you know if repeat victim?	YES	NO	UNSURE
Description of the e-Safety incident: *(please give as much information as you are able – use the prompts overleaf in the guidance)*					
Description of information recorded or secured **(please refer to legal guidance overleaf)** Have files, audio/text/images been recorded and secured? Has any computer or other technology including phones been secured?			YES	NO	
If yes, how and where, who by and when?					
What actions were taken, and by whom? *Give details of agencies informed and contact person within those agencies*.					
Name of person completing this form:		Organisation:			
Date:		Signature			



e-Incident Log Sheet 1 – "member of staff identifying incident" – guidance

Date and Time section:

Please complete all sections, if you don't know the exact day or time of the incident, please write 'unknown'

Description of the e-safety incident:

It is vital that all details you know are recorded, including how the information became known to you and from whom. If there is insufficient space on the form, please use additional sheets, but ensure that they are firmly attached and a note clearly identifies additional sheets used. Include detail of specific services or websites used if known (e.g., chat room, instant messenger); e-mail addresses; usernames etc. Give full details of real names and e-mail addresses etc where known. Some prompts to assist you could be:

How was the incident identified? Who was involved and how do you know this? Why do you have concerns?

Description of information recorded or secured

Legal guidance for those reporting e–Safety incidents that involve a criminal offence POWERS

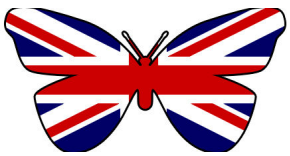
If **any person** has reasonable grounds to believe that an offence IS being committed, then they may **detain the person (offender only)** and **secure any evidence** of the offence (including property). This would include the property of a victim or offender. Once evidence is secured the Police may then seize the property under the Police & Criminal Evidence Act 1984.

Offences committed via computers/laptops/mobile phones.

In these situations the securing of information **must be carried out in a specific way** in order to obtain the best evidence possible for the police and other law enforcement agencies. When a computer is turned on or on standby it should be **left exactly as it is**; in order to allow a trained seizure officer to attend. In all cases; attempts should be made to **record in note form** any details that can be seen on the screen. **DO NOT follow any links or change any pages**.

Information that should be noted if on screen:

- Website address.
- Email addresses of sender and recipient.
- Dates and Times.
- User names.

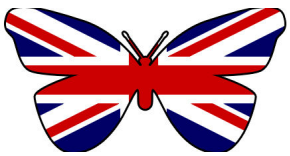


- Mobile phone numbers.
- Any profile information.
- Any text from chat conversations.

If a request for inappropriate behaviour is made on FACEBOOK, any chat forum or social networking site. **DO NOT DELETE or interfere with the offending account**, (this will be done when the evidence is secured). This will enable the police to conduct their enquiries expediently and facilitate the speedier return of seized computer equipment to their owners.
The above information is not an exhaustive list and any other information noted on screen should be included.

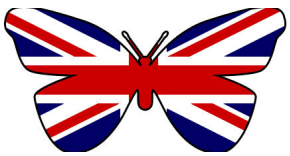
Actions taken

Please give full details of other agencies that have been informed. If the police have not been informed, this must be noted, together with reasons, as e-safety incidents extend well beyond 'grooming' and may be linked to other criminal activity. This may include racist incidents, radicalisation or bullying online, please see legal framework section 4.2 for a comprehensive list. The form must then be signed and dated and handed as soon as possible to the person responsible for child protection within your organisation



e-Incident Log Sheet 2 – “Notifications and Actions” – front cover

To be completed by the person with responsibility for child protection within the organisation		
Notifications: 1. Was notification to the Local Authority Designated Officer required? 2. 2. If yes, what was the outcome? 3. Have you notified the police? 4. Please give details with **reference to guidance overleaf**. **NB This is not an exhaustive list there may be other actions you are required to carry out within your specific organisation.**	YES	NO
Conclusion to the incident:		
Have specific vulnerabilities or trends been identified? If ‘yes’ what action will be taken?		
Name of person completing this form: Organisation: Date: Signature		



e-Incident Log Sheet 2 – “Notifications and Actions” - person with responsibility for child protection

Notifications

Please give full details of other agencies that have been informed. The person initially identifying the incident may have already contacted others, please also record them here, plus any additional action taken by you after receiving the completed Log Sheet 1.

As with Log Sheet 1, if the police have not been informed, this must be noted, together with reasons, as e- safety incidents extend well beyond ‘grooming’ and may be linked to other criminal activity. This may include racist incidents, radicalisation or bullying online, please see legal framework section 4.2 for a comprehensive list.
It is possible that information has not been recorded and secured by the member of staff completing Log Sheet 1. You are reminded that you have powers to detain and secure if you have reasonable grounds to believe that an offence IS being committed. You may **detain the person (offender only)** and **secure any evidence** of the offence (including property). This would include the property of a victim or offender.

Once evidence is secured the Police may then seize the property under the Police & Criminal Evidence Act 1984.

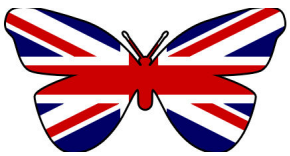
Offences committed via computers/laptops/mobile phones.

In these situations the securing of information **must be carried out in a specific way** in order to obtain the best evidence possible for the police and other law enforcement agencies.

When a computer is turned on or on standby it should be **left exactly as it is**; in order to allow a trained seizure officer to attend. In all cases; attempts should be made to **record in note form** any details that can be seen on the screen. **DO NOT follow any links or change any pages**.

Information that should be noted if on screen

- Website address.
- Email addresses of sender and recipient.
- Dates and Times.
- User names.
- Mobile phone numbers.
- Any profile information



- Any text from chat conversations.

If a request for inappropriate behaviour is made on FACEBOOK, any chat forum or Social networking site. **DO NOT DELETE or interfere with the offending account**, (this will be done when the evidence is secured). This will enable the police to conduct their enquiries expediently and facilitate the speedier return of seized computer equipment to their owners. The above information is not an exhaustive list and any other information noted on screen should be included.

Conclusion to the incident

Please record any disciplinary action taken or communications with parents or carers, as well as specific detail of future meetings, monitoring or discussion planned.

Vulnerabilities and Trends

If there are additional vulnerabilities and trends that have been revealed by the incident, there may be a need to review organisational policy or pass information to other agencies at a later date, either once the investigation has been concluded or even before that. Please record all details that you are able to provide at this stage.