ROSEMARY WORKS E-SAFETY POLICY

POLICY DOCUMENT	**Policy 2017**
STATUTORY	**Statutory**
Legislation: Education/Other	E-Safety
Lead Member of Staff	Rob Dell
Lead Board Member	Jacqueline Logue
Publication /Revision Date	26th May 2016
Approved by	Monthly Management Meeting
Approval Date	8th June 2016
Full Board Ratification Date	
Review Frequency	1 years
Date of next review	June 2017
Publication date: **School Website** **Staff Information folder**	28th June 2017
Chair of Board signature	
Purpose	To ensure that the Head teacher and The Board of Directors act in accordance with the law on Data protection
Supporting documents	Data Protection Act 1998 Fair Processing Notices (Appendix 2 and 3)

Rosemary Works School e-safety policy

Introduction

TEACHING AND LEARNING

- Why Internet use is important
- Internet use will enhance learning
- Pupils will be taught how to evaluate Internet content

MANAGING INFORMATION SYSTEMS

- Information systems security
- Management of e-mail
- Management of published content and school website
- Publishing pupil’s images and work
- Social networking and personal publishing
- Managing Filtering
- Managing emerging technologies
- Protecting personal data

POLICY DECISIONS

- Authorising Internet Access
- Assessing risks
- Handling e-safety complaints
- Community use of the Internet

COMMUNICATIONS POLICY

- Introducing the policy to pupils
- Staff and the e-safety policy
- Enlisting parents’ support

Appendix A – Referral Process
Appendix B – KS1 and KS2 E-Safety Rules
Appendix C – Parental/Pupil Consent Forms
Appendix D – Staff Acceptable Use Policy

E-Safety Policy

Introduction

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- National Education Network standards and specifications.

The e-Safety Policy and its implementation will be reviewed annually.

TEACHING AND LEARNING

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- 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 needs of the curriculum.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils’ age and maturity.
- 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 taught how to evaluate Internet content

- The schools will endeavour to ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- As pupils begin to use the Internet for research purposes they will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of every subject.

Management of e-mail

- Users may only use approved e-mail accounts.
- Users must immediately tell a teacher if they receive offensive e-mail.
- Users must not send jokes or other materials that the receiver may find offensive
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group email addresses should be used in school.
- Access in school to external personal e-mail accounts should be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Management of published content and school website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

(see Mobile Phones Policy and Use of Children's Photographs Policy)

Social networking and personal publishing

- The school will block access to social networking sites and newsgroups will be blocked unless a specific use is approved.
- **Pupils and staff will be advised never to give out personal details of any kind which may identify themselves or others and / or their location.**
- The prevention of cyber bullying will be taught at the appropriate times according to age group and the range of access to the internet the children are exposed to. If any cases of cyber bullying are reported or observed, we will follow the school's behaviour management procedure (see policy).

Managing Filtering

- The school will work with ICT Solutions to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the Head Teacher or Child Protection Officer
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

POLICY DECISIONS

Authorising Internet Access

- All staff must read and sign the 'Staff Code of Conduct for ICT' and read the guidance before using any school ICT resource.
- At Key Stage 1 and Foundation Stage, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised Internet access.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaints about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

COMMUNICATIONS POLICY

Introducing the policy to pupils (in KS2)

- E-Safety rules will be posted in appropriate classrooms with Internet access.
- Users will be informed that network and Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.

Staff and the e-safety policy

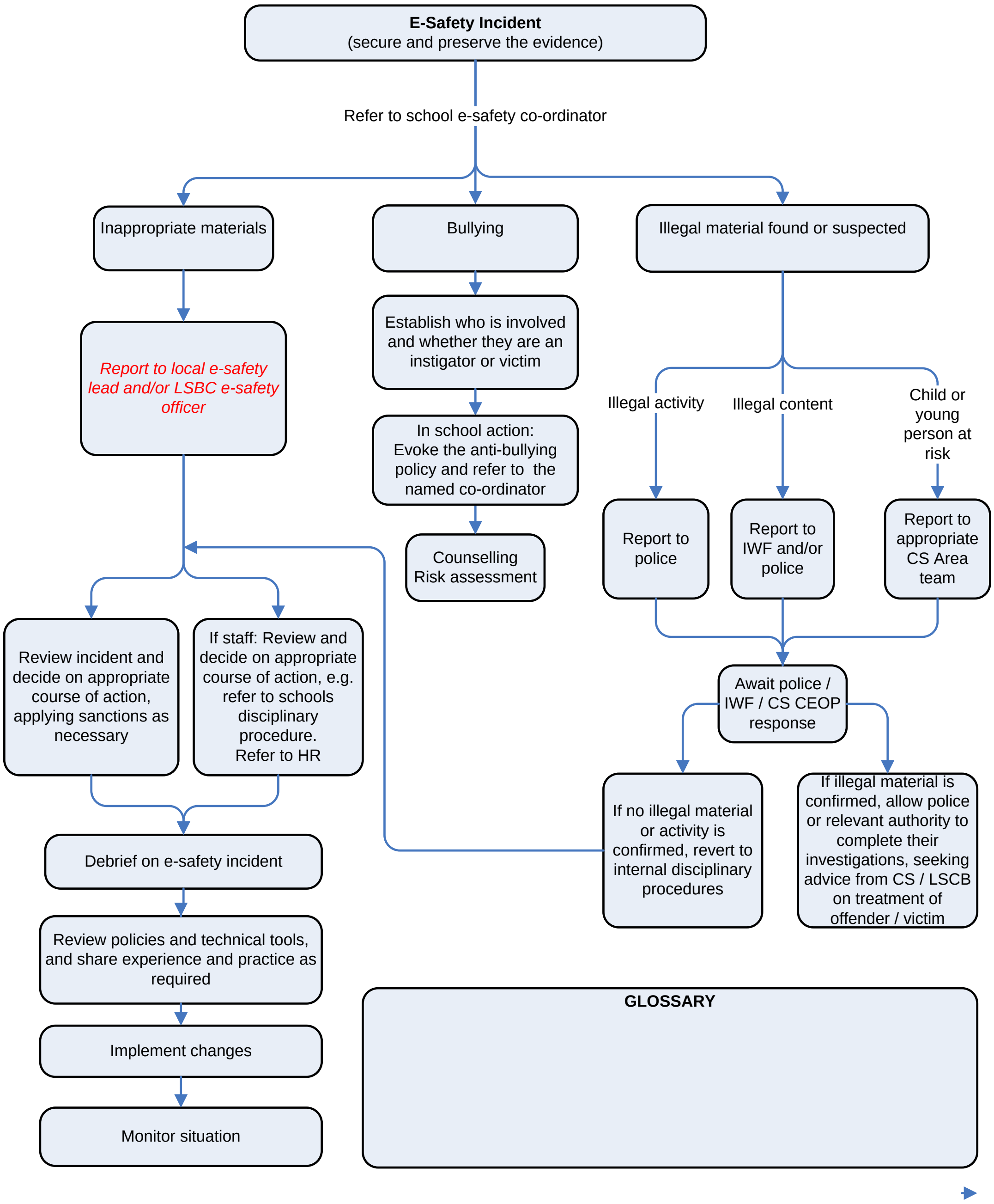
- All staff will be given the School e-Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents’ support

- Parents’ attention will be drawn to the school’s e-Safety Policy in newsletters and on the school website.

DRAFT

Flowchart for responding to e-safety incidents concerning children


E-Safety Incident
(secure and preserve the evidence)
Refer to school e-safety co-ordinator
Inappropriate materials
Bullying
Illegal material found or suspected
Report to local e-safety lead and/or LSBC e-safety officer
Establish who is involved and whether they are an instigator or victim
In school action: Evoke the anti-bullying policy and refer to the named co-ordinator
Counselling Risk assessment
Illegal activity
Illegal content
Child or young person at risk
Report to police
Report to IWF and/or police
Report to appropriate CS Area team
Await police / IWF / CS CEOP response
Review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: Review and decide on appropriate course of action, e.g. refer to schools disciplinary procedure. Refer to HR
If no illegal material or activity is confirmed, revert to internal disciplinary procedures
If illegal material is confirmed, allow police or relevant authority to complete their investigations, seeking advice from CS / LSCB on treatment of offender / victim
Debrief on e-safety incident
Review policies and technical tools, and share experience and practice as required
Implement changes
Monitor situation
GLOSSARY

Rosemary Works School

e-Safety Rules for KS2

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil: ***Class:***

Pupil’s Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computers, network, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed: ***Date:***

Parent’s Consent for Web Publication of Work and Photographs

I agree that my son/daughter’s work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent’s Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: ***Date:***

Please print name:

Please complete, sign and return to the school.

Rosemary Works School

e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil: ***Class:***

Parent’s Consent for Web Publication of Work and Photographs

I agree that my son/daughter’s work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent’s Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: ***Date:***

Please print name:

Please complete, sign and return to the school.

To ensure that members of staff are fully aware of their professional responsibilities when using information and communication systems equipment staff are asked to sign this code of conduct. Members of staff must read and understand the school's e-safety policy prior to signing.

I understand that the school ICT equipment and systems are the property of the school whether used on or off the premises.

I understand that it is a disciplinary offence to use any school ICT system or equipment for a purpose not permitted by its owner. The Head Teacher will provide clarification.

I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras; email and social networking. ICT use may also include personal ICT devices with the permission of the Head Teacher if used for school business.

I understand that school information systems and equipment may not be used for private purposes without permission from the Head Teacher.

I understand that my use of school information systems, Internet and email is monitored and recorded to ensure policy compliance.

I will respect system security and I will not disclose or share any password or security information to anyone other than the Head Teacher.

I will not install any software or hardware without permission.

I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding the inappropriate use of ICT systems or equipment to the Designated Child Protection Officer or Head Teacher.

I will ensure that all electronic communications that I make are compatible with my professional role.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.