Robinsfield Infant School

Behaviour Policy

Reviewed by: Lorraine Wood and Will Byard

Date: May 2017

Review due: May 2018

E-SAFETY POLICY

CONTENTS

1. The Technologies

1.1 ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information.
Current and emerging internet and online technologies can be accessed using a range of devices including smart phones, PCs, tablets, smart TVs and games consoles. These internet and online technologies used in school and, more importantly in many cases, used outside of school by children may include:

- The internet
- World Wide Web
- email
- Instant messaging (e.g. Instant Messenger)
- Web based voice and video calling (e.g. Skype)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. YouTube)
- Music and video downloading (e.g. iTunes)

2. Our Whole School Approach to the Safe Use of ICT

2.1 Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive e-Safety education programme for pupils, staff and parents

3. Roles and Responsibilities

3.1 E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school.

4. Leadership Team

4.1 The Senior Leadership Team (SLT) ensures that the Policy is implemented and compliance with the Policy monitored. Schools should include e-Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use.

5. Network Manager

5.1 Abdul Akodu (Whole School Network Manager) maintains and updates the site lists within the web appliance.

6. e-Safety Co-ordinator

6.1 Our school e-Safety Co-ordinator is Will Byard (Computing Lead).

He ensures they keep up to date with e-Safety issues and guidance. The school's e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

7. Governing Body

7.1 The Governing Body needs to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.

8. School Staff

8.1 All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures.

Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the school's Acceptable Use Policy including:

- Safe use of email;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of children's photos and work on the website;
- e-Bullying/Cyberbullying procedures;
- Their role in providing e-Safety education for pupils;

Staff are reminded/updated about e-Safety matters at least once a year.

9. Pupils

9.1 Pupils are expected to take an active part in planned lessons, e-Safety activities to support their understanding and confidence in dealing with e-Safety issues, both at home and school. Pupils are expected to follow the school's policy on the acceptable use of the equipment and the Internet.

Policy introduction to pupils

- Rules for Internet access are taught to all pupils;
- Pupils/staff/all users will be informed that internet use will be monitored;
- Instruction in responsible and safe use should precede internet access;
- A module on safe internet use will be included in the PSHCE (Personal, Social, Health, Cultural Education)/Computing programme at the beginning of each school year, covering both school and home use

10. Parents

10.1 Parents are given information about the school's e-Safety policy at the Admission interview and are signposted to a copy of this on the school's website.

During e-Safety week there will be an opportunity for parents to attend an e-Safety workshop where they will have the chance to ask questions and find out more about keeping their children safe on the Internet at home.
Internet issues will be handled sensitively to inform parents/carers without undue alarm;
A partnership approach with parents/carers will be encouraged. This includes:

- Demonstrations practical sessions and suggestions for safe internet use at home;
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents/carers;

- Interested parents/carers will be referred to relevant organisations

Technical and hardware guidance

11. Content Filter

11.1 The school is part of the London Grid for Learning (LGfL) network and thus we can ensure that most inappropriate content is blocked. While this is the case, the content filter cannot block 100% of inappropriate material thus adults in school need to exercise diligence when using ICT with children.

12. Unsuitable Material

12.1 Despite the best efforts of the LGfL filter, Network Manager and school staff, occasionally pupils may come cross something on the internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

12.2 The action will include:

- Making a note of the website and any other websites linked to it and inform the Network Manager straight away.
- The Network Manager will then add the website to the blocked list in the Sophos system and inform the member of staff, e-Safety Co-ordinator and the head teacher.
- Discussion with the pupil about the incident, and how to avoid similar experiences in future

12.3 Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

13. Downloading Files and Applications

13.1 The internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

- Pupils and staff are not allowed to download any inappropriate or unsuitable material from the internet.
- Staff and pupils are not allowed to download files through email other than using their LGfL staff account.

13.2 The school has a system whereby only authorised staff can install software onto devices as an administrator password is needed.

14. Portable Storage Media

14.1 Portable media USB memory sticks are a common way of introducing a virus or other undesirable agent into a school computer system. Staff will not use external media storage devices.

15. Security and Virus Protection

15.1 The school uses Sophos software. The software is monitored and updated regularly by the Network Manager.

Any software messages or pop-up screens reporting evidence of viral infection should **always** be reported immediately to the Network Manager via email.

16. E-Safety for Pupils

16.1 We believe it is our responsibility to prepare pupils for their lives in the modern world, and ICT is an integral part of that world. At our school we are committed to teaching pupils to use the ICT effectively and appropriately in all aspects of their education.

17. Internet Access at School

17.1 Access for all - Inclusion

All pupils have access to the internet as part of the curriculum. Details of how we manage access to the curriculum for all pupils is contained in our SEND Policy

17.2 Use of the internet by Pupils

Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the internet.

18. Out of Hours Provision

18.1 There will be no unsupervised access to the internet at any time during Out of Hours provision.

19. Using the internet for Learning

19.1 The internet is an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials.

19.2 We teach all of our pupils how to find appropriate information on the World Wide Web, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

- Teachers carefully plan all web-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.
- Children are only allowed to use selected search engines (e.g. KidRex) that deliver highly filtered results.
- Staff have access to search engines such as Google, but only use the search engines available to children when searching in front of children.
- Staff are made aware that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

20. Teaching Safe Use of the Internet and ICT

20.1 It is crucial to teach pupils how to use the internet safely, both at school and at home, and we use the Kidsmart safety code to support our teaching in this area:

Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES. Materials from CEOP will also be used to support teaching and e-Safety activities.

http://www.childnet.com/
https://www.thinkuknow.co.uk/parents/

20.2 The main aspects of this approach include the following five SMART tips:

Safe - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online.
Meeting someone you meet in cyberspace can be dangerous. Never arrange to meet anyone you have met on the internet.
Accepting emails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages.
Remember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation.
Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

21. Suitable Material

21.1 We encourage pupils to see the internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. With younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

21.2 We believe it is better to support children in finding their way around the internet with guidance and positive role modelling rather than restrict internet use to strict curriculum based research.

As well as internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in free time at out-of-school-hours provision, and at home.

22. Using email at School

22.1 Email is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of email, and how to use it appropriately and effectively.

- We teach the use of email as part of our Computing curriculum, and use it across the curriculum in a range of ways.
- Pupils are taught that email messages sent using a school account will represent the school as well as the pupil, and that they should take care to act respectfully and appropriately
- We only use email that goes through LGfL, as this is carefully monitored and controlled (see 11).
- Pupils and staff are unable to access personal email using school Internet facilities, due to the quantity of unsolicited email (Spam), unsuitable content and virus threats associated with commercial email accounts.

23. Chat, Discussion and Social Networking Sites

23.1 These forms of electronic communication are increasingly used by pupils out of school, and can also contribute to learning across a range of curriculum areas.

23.2 Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media. We use the resources, guidelines and materials offered by CEOP and LGfL.

- We believe that public chatrooms are unsuitable for the age of our pupils. Pupils are unable to access public chat rooms (e.g. MSN) using school resources.
- We believe that social media sites are unsuitable for the age of our pupils. Pupils are unable to access social media sites (e.g. Facebook, Twitter, Club Penguin) using school resources.

24. Internet-enabled devices

24.1 Pupils will be taught the legal and moral implications of posting photos and personal information to public websites and how the data protection and privacy laws apply using age appropriate language.

- Pupils are not allowed to have personal mobile phones or other similar devices in school.
- Pupils and parents are asked not to use their mobile phones on the school site.
- For all performances, parents are asked not to film and are reminded to not upload images and films of children to a public website, e.g. Facebook.

25. Cyberbullying - Online bullying and Harassment

25.1 Online bullying and harassment such as through instant messaging, mobile phone texting or email, are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy.

These include:

- No access to public chat-rooms, Instant Messaging services.
- Pupils are taught how to use the internet safely and responsibly, and are given access to guidance and support resources from a variety of sources.
- We work with parents to help them understand the potential dangers of having access to technology that can be used for cyberbullying at this age.

25.2 We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

26. Contact Details and Privacy

26.1 Pupil's personal details, identifying information, images or other sensitive details will never be shared or placed in a public forum unless written permission has been obtained from a parent or legal guardian.

Pupils are taught that sharing this information with others can be dangerous.

Permission is sought from parents to use photographs of children for the school website when they are enrolled into school. Images of pupils never appear alongside their name.

27. Deliberate Misuse of the Internet Facilities

27.1 Pupils are taught to use the internet appropriately and safely.

27.2 Incident of pupils found to be deliberately accessing inappropriate content will be dealt with in line with our behaviour policy.

28. How will complaints regarding e-Safety be handled?

28.1 It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

28.2 Because of the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of internet access.

28.3 Staff and pupils are given information about infringements in use and possible sanctions.

Over and above sanctions put in place in line with the school's behaviour policy, the following may be necessary:

- Informing parents or carers
- Referral to LA / Police

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the head teacher. Any complaint about head teacher misuse is referred to the school governor responsible for monitoring safeguarding, as detailed in the school safeguarding policy.

29. Data Protection Policy

29.1 Our school is aware of the data protection law as it affects our use of the internet, both in administration and teaching and learning.

We adhere to the national guidelines on data protection.

Staff understand the legal and disciplinary implications of using the internet at school for illegal purposes.

Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the internet by members of the school community.

Robinsfield e-Safety agreement form: parents

Parent / guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the internet and other ICT facilities at school.

I know that my daughter or son is aware of e-safety and have discussed how to use ICT responsibly in school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the web sites they visit, and that if they have concerns about their e-safety or behaviour that they will contact me.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent / guardian signature: _____

Date: ___/___/___

Use of digital images - photography and video: I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital images - photography and video'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.

Parent / guardian signature: _____ Date: ___/___/___

Use of digital images - photography and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity;
  e.g. photographing children at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the children to see their work and make improvements.

- Your child's image for presentation purposes around the school;
  e.g. in school wall displays and presentations to capture images around the school or in the local area as part of a project or lesson.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a DVD or a document sharing good practice; in our school prospectus, magazine or on our school website. In rare events, your child's could appear in the media if a newspaper photographer or television film crew attend an event.

If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Further information for parents on e-Safety can be found at:

UK Safer Internet Centre
https://www.saferinternet.org.uk/

London Grid for Learning Online Safety and Safeguarding
https://www.lgfl.net/online-safety/

Child Exploitation and Online Protection Command
https://ceop.police.uk/safety-centre/

Further information for parents and carers

For more information on how to keep your child safe online please visit these website.

UK Safer Internet Centre Parents Guide to Technology
https://www.saferinternet.org.uk/advice-centre/parents-and-carers/parents-guide-technology

London Grid for Learning Online Safety and Safeguarding
https://www.lgfl.net/online-safety/

Child Exploitation and Online Protection Command
https://ceop.police.uk/safety-centre/