



Living our learning

Knowles Primary School
Queensway
Bletchley
Milton Keynes
MK2 2HB

Tel: 01908 373588

Web: www.knowlesprimaryschool.org.uk

Headteacher: Mrs Gi Sierant

e-Safety Policy

Date agreed by the Governing Body: 29th June 2016

Date distributed to staff: 5th July 2016 (Z Drive)

Date to be reviewed: (Every year) June 2017

Knowles Primary School takes the safety of all children and adults very seriously. This policy is written to protect all children and adults. We recognise that E-Safety encompasses not only Internet technologies, but also electronic communications such as mobile phones and wireless technology.

What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs);
- Internet research: websites, search engines and web browsers;
- Mobile phones
- Internet communications: e-mail and IM;
- Webcams and videoconferencing;
- Wireless games consoles.

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used. This e-Safety Policy recognises the skills that children and young people need to develop when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

The risks to children and adults are caused by people acting inappropriately or illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity.

What are the risks?

Receiving inappropriate content;
Predation and grooming;
Requests for personal information;
Viewing 'incitement' sites;
Bullying and threats;
Identity theft;
Publishing inappropriate content;
Online gambling;
Misuse of computer systems;
Publishing personal information;
Hacking and security breaches;
Corruption or misuse of data.

A summary of our school's safety responsibilities is outlined below. This list will assist in developing a co-ordinated and effective approach to managing e-safety issues.

Designated Safeguarding Lead: Sarah Hilton

Deputy Safeguarding Lead: Gi Sierant

Safeguarding Officers: Sarah Rice
Doll Downard
Sam Searle
Sorrell Yates

Computing Coordinator: Simone Lines

E-Safety Designated Lead: Sarah Hilton

E-Safety Team: Paul Heather
Simone Lines
Helen Loftus

- The roles of the e-Safety/computing Coordinator, along with the Designated Safeguarding Lead may overlap. The e-safety Co will receive support and advice from the **county e-Safety Officer**, and where necessary, the Police.
- The e-Safety/computing coordinator should maintain the e-Safety Policy, manage e-Safety training and keep abreast of local and national e-Safety awareness campaigns.
- Knowles Primary School will review the policy regularly and revise the policy annually to ensure that it is current and considers any emerging technologies.
- Knowles Primary School will audit their filtering systems regularly with LGFL to ensure that inappropriate websites are blocked.
- To ensure that pupils and staff are adhering to the policy, any incidents of possible misuse will be investigated.
- Knowles Primary School will include e-Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem. We use the SAFE materials to carry this out.
- All staff must read and sign the Acceptable Use Policy.
- Parents, children and the Headteacher should sign and return the e-Safety Rules consent form.
- The e-Safety Policy will be made available to all staff, governors, parents and visitors through the website.

Implementation and Compliance

No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences.

How can Internet use enhance learning?

- Knowles Primary School's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Knowles Primary Schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to online 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 to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Teaching and learning

Why is Internet use important?

Developing effective practice in Internet use for teaching and learning is essential. The purpose of Internet use in Knowles Primary School is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance Knowles Primary School's management functions. The Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is an essential element in 21st century life for education, business and social interaction. Knowles Primary School has a duty to provide students with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security. Our 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.

- 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.

Evaluating Internet Content

Inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher. Knowles Primary School will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Local Area Network security

- Users must act reasonably;
- Users must take responsibility for their network use. For all staff, flouting electronic use policy is regarded as a matter for dismissal;
- Workstations should be secured against user mistakes and deliberate actions, e.g. deleting files and folders;
- Servers will be located securely and physical access restricted;
- The server operating system will be secured and kept up to date;
- Virus protection for the whole network will be installed and current;
- Access by wireless devices must be pro-actively managed.

Wide Area Network (WAN) security

Connectivity to be procured in line with government guidelines and guidance. Firewalls and switches are configured to prevent unauthorised access between schools.

- The security of Knowles Primary School information systems will be reviewed regularly;
- Virus protection will be updated regularly and recorded.
- Security strategies will be discussed with the LA when necessary;
- Personal data sent over the Internet should be encrypted or otherwise secured;
- Portable media may not be used without specific permission followed by a virus check;
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail;
- Files held on Knowles Primary School's network will be regularly checked;
- The ICT co-ordinator / network manager will review system capacity regularly.

How will email be managed?

- Whole class or teacher email addresses will be used in Knowles for communication outside of Knowles Primary School by children.
- Pupils may only use approved email or blogging accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Access in school to external personal email accounts may be blocked.
- The forwarding of chain messages is not permitted.
- Pupils must immediately tell a teacher if they receive offensive e-mail;
- Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team

How will published content be managed?

- We have created a website that inspires pupils to publish work of a high standard.
- We use it to celebrate pupils work, promote Knowles Primary School and publish resources for projects.
- Publication of information should be considered from a personal and school security viewpoint.
- The contact details on the website should be Knowles Primary School address, email and telephone number. Staff or pupils' personal information must not be published.
- The Headteacher in conjunction with Network Manager will take overall editorial responsibility and ensure that content is accurate and appropriate and editorial guidance will help reflect Knowles Primary School's requirements for accuracy and good presentation.
- The website will comply with current guidelines for publications including respect for intellectual property rights and copyright.

School Website and Learning Platform

The contact details on the website should be Knowles Primary School address, e-mail and telephone number. Staff or pupils' personal information must not be published. E-mail addresses should be published carefully, to avoid spam harvesting. The Headteacher in conjunction with Network Manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

Use of Images

Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless there is parental permission. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Knowles Primary School reserves the right to publish any images. Parents and carers can register their right to refuse images of their children being electronically published by contacting the headteacher.

Social Networking

- Knowles Primary School will block/filter children's access to social networking sites;
- Newsgroups will be blocked unless a specific use is approved;
- Children will be taught about the role of CEOP (Child Exploitation and Online Protection) and how to contact such organisations:
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space;
- They should consider how public the information is and consider using private areas;
- Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school;
- **Teachers should be advised not to run social network spaces for student use on a personal basis.**

How will filtering be managed?

- Knowles Primary School will work with broadband provider 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 ICT co-ordinator or a senior member of staff, and the incident recorded in the safety incident log.
- Knowles Primary School's broadband access includes filtering appropriate to the age and maturity of pupils. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that staff believe is illegal must be reported to the Headteacher who will inform the appropriate agencies.

- We keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies.
- Mobile Phones should be stored away during teaching hours and access to them will only be done when authorized by a senior member of staff.
- Abusive messages should be dealt with under Knowles Primary School's behaviour and anti-bullying policy.
- Emerging technologies will be examined for educational benefit and the Headteacher in consultation with staff will give permission for appropriate use.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- Pupils are not allowed to bring mobile phones into school. Under certain circumstances exceptions can be discussed with the Headteacher, so that pupil mobile phones can be kept in Knowles Primary School office. Parents must complete the permission slip to acknowledge that Knowles Primary School takes no responsibility for phones which are left in the office.

Video Conferencing

School videoconferencing equipment should not be taken off school premises without permission because use over the non-educational network cannot be monitored or controlled. At present no video conferencing facilities exist in school.

Users

Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure. Pupils should ask permission from the supervising teacher before making or answering a videoconference call. Videoconferencing should be supervised appropriately for the pupils' age. Parents and guardians should agree for their children to take part in videoconferences, probably in the annual return.

Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Mobile phones will not be used during lessons or formal school time. All pupil mobile phones will be handed into the office before registration and collected at the end of the day. Only pupils who walk to school or home independently will be able to bring a phone to school. The sending of abusive or inappropriate text messages is forbidden.

Personal Data

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

Internet Access

- Knowles Primary School will maintain a current record of all staff and pupils who are granted access to Knowles Primary School's electronic communications;
- All staff must read and sign the 'Staff acceptable use policy before using any school ICT resource;

Internet Risks

Knowles Primary 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 Knowles Primary School nor our Local Educational Authority can accept liability for the material accessed, or any consequences resulting from Internet use.

Knowles Primary School will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

How will e-Safety complaints be handled?

- Complaints of Internet misuse will be dealt with under Knowles Primary School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the Head of School. If the complaint is about the Head of School this should be reported to the Chair of Governors.
- All e-Safety complaints and incidents will be recorded by Knowles Primary School — including any actions taken.
- Pupils and parents will be informed of the complaints procedure. Parents and pupils will work in partnership with staff to resolve issues.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to Knowles Primary School's disciplinary and child protection procedures.

How is the Internet used across the community?

- We recognise that children can access the internet outside of school and offer support and advice to parents on internet safety through regular information sent home with children and through advice on our website.
- Knowles Primary School will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

How will Cyberbullying be managed?

- Cyberbullying is defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.
- It is essential that pupils, members of staff and parents/carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse.
- Promoting a culture of confident users will support innovation and safety. DCSF and Childnet have produced resources and guidance that will be used to give practical advice and guidance on cyberbullying: <http://www.digizen.org/cyberbullying>
- Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents of cyberbullying reported to Knowles Primary School will be recorded.
- There are clear procedures in place to investigate incidents or allegations of bullying:
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- Knowles Primary School will take steps to identify bullying behaviour, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include: The perpetrator will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period of time.
- Parent/carers will be informed and the Police will be contacted if a criminal offence is suspected.

Other E-safety Issues

Sexting: Children in Year 5 and 6 will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the world wide web.

Pornography: many children will come across some type of pornographic content when searching the Internet. Children are taught about what to do if they come across this type of material and who to speak to.

How will the policy be introduced to pupils?

- At Knowles we teach about e–Safety as a computing lesson activity and as part of every subject whenever pupils are using the internet.
- Pupil instruction in responsible and safe use should precede Internet access every time they go online.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

We will use the following e–Safety programmes:

Think U Know: www.thinkuknow.co.uk Childnet: www.childnet.com Kidsmart: www.kidsmart.org.uk Safe Social Networking: www.safesocialnetworking.com

How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff and published on Knowles Primary School Learning Platform.
- To protect all staff and pupils, Knowles Primary School will implement Acceptable Use Policy. Staff should be aware that Internet traffic can be monitored and traced to the individual user; discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use both professionally and personally will be provided, both internally and externally.

How will parents' support be enlisted?

- Parents' attention will be drawn to Knowles Primary School e–Safety Policy in newsletters, Knowles Primary School brochure and on Knowles Primary School website.
- A partnership approach with parents will be encouraged. This will include parent meetings with demonstrations and suggestions for safe home Internet use.
- Parents and children will be requested to sign an e–Safety/internet agreement as part of Knowles Primary School's on entry procedures. Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Policy Management

This policy is linked to the following mandatory school/centre policies: Safeguarding, Child Protection, Whistle Blowing, Health and Safety, Behaviour and Bullying, Home School Agreements, ICT and PHSE.

Who will review the policy?

The e–Safety Policy and its implementation will be reviewed annually. This policy should be reviewed annually by SLT and Governors.