ST BRIDGET'S C of E PRIMARY SCHOOL

E-Safety & Acceptable Use Policy

Policy Written January 2018

CRC Links

Article 13. Children have the right to get and share information, as long as the information is not damaging to them or others. In exercising the right to freedom of expression, children have the responsibility to also respect the rights, freedoms and reputations of others. The freedom of expression includes the right to share information in any way they choose, including by talking, drawing or writing.

Article 16. Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.

Article 17. Children have the right to get information that is important to their health and well-being. Governments should encourage mass media – radio, television, newspapers and Internet content sources – to provide information that children can understand and to not promote materials that could harm children. Mass media should particularly be encouraged to supply information in languages that minority and indigenous children can understand. Children should also have access to children's books.

Article 19. Children have the right to be protected from being hurt and mistreated, physically or mentally.

Article 28. Right to education – Every child has the right to an education.

Article 29. Goals of education - Your education should help you use and develop your talents and abilities. It should also help you learn to live peacefully, protect the environment and respect other people.

Article 31. Children have the right to relax and play, and to join in a wide range of cultural, artistic and other recreational activities.

National guidance suggests that it is essential for schools to take a leading role in e-safety.

Becta in its "Safeguarding Children in a Digital World" suggested: "That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT too."

The Byron Review "Safer Children in a Digital World" stressed the role of schools: "One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."

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.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others.

The safety of children at St Bridget's C of E Primary School is of the utmost importance. Technology is changing at an unbelievable pace and it is our responsibility to ensure that our children have full access to this technology whilst remaining safe and secure. This policy outlines the ways in which we, as a school, advise, protect and safeguard our children, staff and parents from the dangers of technology.

RATIONALE

So as to keep our pupils safe, we at St Bridget's will be implementing this three step approach to E-Safety.

1. **Awareness** – ensuring staff, children and adults are aware of the risks that come with Internet technologies and electronic communications;
2. **Education** – providing staff, children and adults with the knowledge they need to protect themselves and others;
3. **Technology** – implementing systems to protect everybody at St Bridget's.

IMPORTANCE AND BENEFITS OF THE INTERENT USE IN EDUCATION

The purpose of Internet use in school is to raise educational standards, to promote and facilitate student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the Internet in education include:

- access to learning wherever and whenever convenient,
- access to world-wide educational resources, including museums and art galleries,
- educational and cultural exchanges between pupils world-wide,
- access to experts in many fields for pupils and staff,
- professional development for staff through access to national developments, educational materials and effective curriculum practice,.
- collaboration across support services and professional associations,.
- improved access to technical support including remote management of networks and automatic system updates, and
- exchange of curriculum and administration data with the Local Authority.

FILTERING INTERNET CONTENT

In a perfect world, 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.

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

The development in new technology means that unlike ever before children and young people have extensive access to content that could be harmful. The development of the internet has generated a wealth of opportunities for young people to communicate and take up leisure opportunities in a variety of ways e.g. MSN, chat rooms and online gaming. However, these opportunities also have in-built risks in the form of content, contact and conduct. The grid by Hasenbrink, Livingstone, Haddor, Kirwil and Ponte, 2007, as mentioned in the Byron Review, sets out the potentially broad ranging series of risks that the technology of the internet has.

	Commercial	**Aggressive**	**Sexual**	**Values**

Content (Child as recipient)	Adverts Spam Sponsorship Personal information	Violent and hateful	Pornographic or unwelcome sexual content	Bias Racist Misleading information or advice
Contact (Child as participant)	Tracking Harvesting Personal information	Being bullied, harassed or stalked	Meeting strangers, being groomed	Self harm Unwelcome persuasions
Conduct (Child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying and harassing another	Creating and uploading inappropriate material	Providing misleading information and/or advice

These risks are all dependent upon the behaviour of the pupil rather than the technologies themselves. Taking that into consideration, along with the four categories of risks outlined in the above diagram, we at St Bridget's have used this to form the basis for safeguarding our children. Our school Internet filtering system uses these categories when determining which sites are inappropriate. In order to address these risks in school, the following precautions are taken:

Use of an Internet Filter

The filter is provided by Exa (through Hi-Impact) and enables schools full control over allowed and prohibited websites. The filter is pre-configured to prohibit access to any website that falls into one of the categories listed in the previous section. However, this does mean that from time to time, access to important websites that could enhance learning is prohibited. The Headteacher, ICT Leader, ICT assistant and technician all have full control over the filter and are able to have sites blocked or unblocked. They have a responsibility to ensure that no inappropriate content is explicitly permitted.

We accept that some inappropriate content may appear no matter how strictly we monitor the filtering system. Due to this we have developed an "Acceptable Use Policy" which all parents, guardians and children sign upon entry to the school. This document outlines the user's responsibility upon discovering inappropriate material. The pupils' responsibilities are also reviewed and reminded to all pupils regularly through their lessons.

As a continued visual reminder of the E-Safety rules, there will be a poster visible in each room where there is a computer; e.g. ICT suite, classrooms etc. As well as having the posters available within school an age appropriate copy will be sent home with the recommendation that parents/guardians discuss and reinforce these rules and if possible, display the poster in the area of the computer at home. (This will be done annually as part of the new starters pack.)

Monitoring

The use of the Internet can be monitored by the technician. This will enable early notice of inappropriate use by individuals. In such cases, the issue will be dealt with in accordance with the school's behaviour policy.

Restricting Access

At any time, Internet access can be revoked, either individually or for the entire school. Although extreme, this is an essential feature of the network and safeguards against malicious attacks.

COMMUNICATION WITH CHILDREN INCLUDING THE USE OF TECHNOLOGY

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites, forums and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to children and young people including e-mail, home or mobile numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child/young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites .e.g. Facebook, Instagram, Snapchat and Twitter.

Internal e-mail systems should only be used in accordance with the organisation's policy.

This means that adults should:

- Not give their personal contact details to children/young people, including their mobile number.
- Only use equipment e.g. computers, provided by organisation to communicate with children, making sure that parents have given permission for this form of communication to be used.
- Only make contact with children for professional reasons and in accordance with any organisation.
- Recognise that text messaging is rarely an appropriate response to a child in a crisis situation or at risk of harm. It should only be used as a last resort when other forms of communication are not possible.
- Not use internet or web-based communication channels to send personal messages to a child/young person.

(Information taken from 'Guidance for Safer Working Practice for Adults working with Children and Young People'.)

SOCIAL NETWORKING

At St Bridget's, we deny access to all social networking sites for both pupils and staff for personal use within the school context.

The reasons for are as follows:

- Most networking sites have a live chat facility, as well as unfiltered access to potentially inappropriate content. All access is therefore prohibited.
- Children are taught about the risks associated with these sites in their ICT lessons, visiting performance groups and appropriate PSHE or P4C lessons. Many children have access to social networking sites from home. It is therefore essential that they are aware of how to use such sites with care.
- We do not tolerate children attempting to make contact with staff through Social Networking sites.

The exception is as follows:
School uses Facebook and Twitter platforms as a way of communicating to parents and the wider community. School carefully monitor any feedback. Parents are not encouraged to write to school but simply appreciate the children's work and effort.

Advice given to pupils:

- Pupils will be advised never to give out personal details of any kind which may identify them or their location. The risks and dangers of doing this will be highlighted for them.
- Pupils will be advised not to place personal photos on any social network space.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils will be encouraged to invite known friends only and deny access to others.

Advice given to staff:

- Staff are advised not to make contact with current or past pupils via social networking sites.
- To decline any offers of 'friendship' or similar connections on these websites.
- Staff should report to the Headteacher or E-Safety Coordinator if any children try to make contact.

DIGITAL PHOTOGRAPHS AND VIDEOS

Aims

- At St Bridget's we enjoy taking lots of photographs and videos of the pupils going through their daily routine, for example, attending after school clubs, receiving awards, participating in visits or special events. These are then used by staff to celebrate our children's achievements as well as to enhance the school environment as displays.
- To allow activities and events which take place as part of the St Bridget's community to be recorded for posterity to the school and for personal records for parents.

Objectives

- To allow the taking of photographs and the use of videoing to record groups and individuals work and achievements.
- To allow the use of photographs and/or videos within the school premises.
- To allow the use of photographs and/or videos on the Schools VLE and for publicity purposes e.g. in the local paper, School Twitter, School Facebook.
- To have the consent of the parents for this purpose.

Procedure for School and Commercial Use

- To ensure any photographs or video clips used for website purposes do not have the full name of the child by their image.
- If full names are used they are not to have the child's image adjacent to the picture for website purposes.
- Parents have the right to withdraw their child if they do not wish them to be included in any photographs and videos. This would include school performance, assemblies, concerts, sports days and any other school event.
- Only children to whom their parents have previously given permission may have their photographs used. Permission is granted through the 'Home School Agreement' completed on entry to the school.

MOBILE PHONES

Mobile phones pose a significant e-safety risk. This is due to their increasing capabilities to:

- Send MMS (multimedia messages);
- Send SMS (text messages);
- Send and receive video files and images;
- Access the full internet.

So as to minimize these risks, we at St Bridget's have devised a collection of rules and guidelines for pupils and staff.

Children:
Children are not permitted to bring mobile phones to school. The only exception to this rule applies to the children who have brought in written permission from their parents. The mobile phone should then be turned off and handed in to the class teacher so as it cannot be used throughout the school day. However, the school, and any member of staff, will not be held accountable for any damage, loss or theft of the phone whilst on the premises.

Staff and volunteers:
Adults in school may use mobile phones during non-directed time to make personal calls. Non-directed time includes: before school, at lunch-time and after school. Adults should not text or call during lessons/activities where they have a supervisory role. NOTE: Should a member of staff need to be reached, the most effective method is through calling the school office.

If mobile phones are used throughout the school day (for school related communication including Internet access and email) all costs and data charges will not be reimbursed as Internet access and telephones are provided throughout school.

Adults **must not** give out mobile phone numbers to parents on field or residential trips (except SEN reasons) but instead should provide the school office number. The school office will then contact the teacher or member of staff involved.

At no point should a personal mobile phone be used to record images (photograph or video) of a child or children. Instead, if an image or video is needed, a school digital camera must be used.

CYBERBULLING

"Cyberbullying" is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones. It has to have a minor on both sides, or at least have been instigated by a minor against another minor. Once adults become involved, it is plain and simple cyber-harassment or cyberstalking. Adult cyber-harassment or cyberstalking is NEVER called cyberbullying.

The continued targeting of a specific child or group of children by others through the use of ICT is cyberbullying. These actions and behaviours include:

- The use of Social Networking Sites to target children;
- The use of Instant Messaging such as Snapchat and WhatsApp to target children;
- The use of mobile phones to send abusive or threatening messages (either SMS or MMS);

- The use of the Internet to post offensive or derogatory comments;
- Hacking or cracking another person's profile on a website and/or writing comments as though they were that person (fraping)

The E-Safety Coordinator and/or Headteacher must be notified of any occurrences of cyberbullying. It will be entered into the incident log and a formal report will then be made and any punishments will be dealt with in accordance with St Bridget's Anti-Bulling Policy.

SEXTING

The taking and sharing of sexual imagery amongst children forms part of 'Sexting', which is a specific safeguarding issue. This online behaviour is a concern amongst our children and young adults. Knowing how to respond to such an incident is a crucial part of an effective safeguarding approach.

All incidents involving youth produced sexual imagery should be responded to in line with the school's safeguarding and child protection policy. When an incident involving youth produced sexual imagery comes to our schools attention:

- The incident should be referred to the DSL as soon as possible
- The DSL should hold an initial review meeting with appropriate school staff
- There should be subsequent interviews with the young people involved (if appropriate)
- Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm
- At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately.

Securing and Handing Over Devices

Securing and handing over devices to the police. If any devices need to be seized and passed onto the police then the device(s) should be confiscated and the police should be called. The device should be turned off and placed under lock and key (in a Faraday bag) until the police are able to come and retrieve it.

Searching devices, viewing and deleting imagery

Viewing the imagery

Adults should not view youth produced sexual imagery unless there is good and clear reason to do so. Wherever possible responses to incidents should be based on what DSLs have been told about the content of the imagery.

The decision to view imagery should be based on the professional judgment of the DSL and should always comply with the child protection policy and procedures of the school. Imagery should never be viewed if the act of viewing will cause significant distress or harm to the pupil.

If a decision is made to view imagery the DSL would need to be satisfied that viewing:

- is the only way to make a decision about whether to involve other agencies (i.e. it is not possible to establish the facts from the young people involved)
- is necessary to report the image to a website, app or suitable reporting agency to have it taken down, or to support the young person or parent in making a report
- is unavoidable because a pupil has presented an image directly to a staff member or the imagery has been found on a school device or network

Deletion of images

If we as a school decide that other agencies do not need to be involved, then consideration should be given to deleting imagery from devices and online services to limit any further sharing of the imagery. The Searching, Screening and Confiscation advice highlights that schools have the power to search pupils for

devices, search data on devices and delete youth produced sexual imagery. (As stated in the Education Act 2011)

COMMUNICATION OF THE POLICY

Pupils
Rules for Internet access will be posted in the ICT classroom.
Pupils will be informed that Internet use will be monitored.
A list of child friendly sites will be made available, including appropriate search engines.

Staff
All staff will be informed of the School E - Safety Policy and its importance explained.
Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Parents
Parents' attention will be drawn to the School E - Safety Policy in newsletters, the school brochure and on the school Web site.

E-SAFETY RULES

These E-Safety rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school will exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer 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.

CODE OF CONDUCT

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's E - Safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure 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 children's safety to the school E - Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with students are compatible with my professional role.
- I will promote E - Safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of 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.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: .....

Printed: ..... Date: .....

KEYSTAGE 1 E-SAFETY POSTER

These rules help us to stay
safe on the Internet

Think then Click

We only use the Internet when an adult is with us.

We can click on the buttons or links when we know what they do.

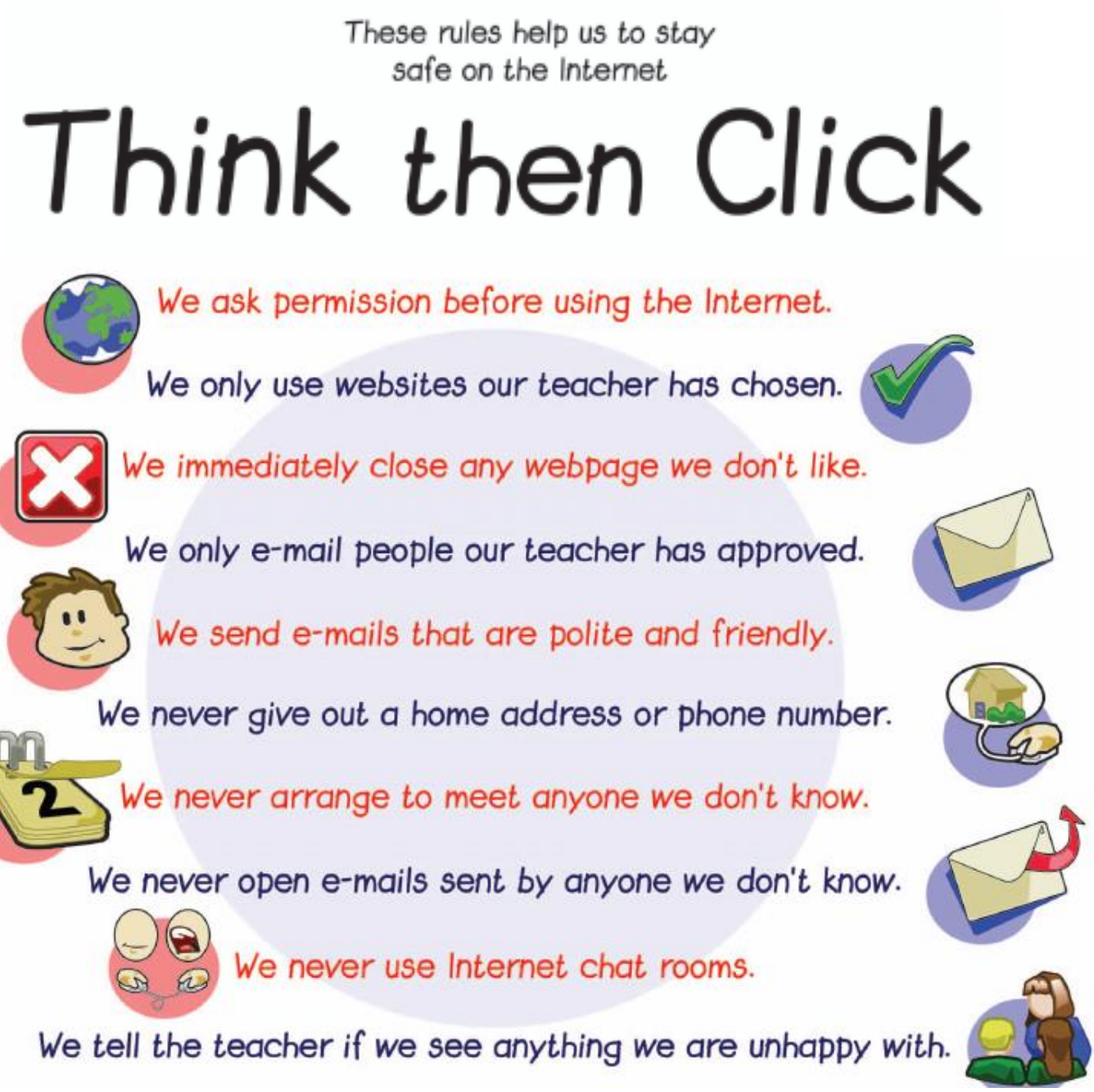
We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

KEYSTAGE 2 E-SAFETY POSTER



USEFUL LINKS

Childnet's 'Using Technology'
http://www.childnet.com/teachers-and-professionals/for-you-as-a-professional/using-technology
The Professional Online Safety Helpline
http://www.saferinternet.org.uk/professionals-online-safety-helpline
Advice for Professionals
https://www.kidscape.org.uk/advice/advice-for-professionals/
Sexting in Schools and Colleges
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

REVIEW

Written by Mrs Emma Johnson January 2017

This policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

The Headteacher and staff will review this policy in accordance with the development priorities stated in the School's Development Plan. Any suggested amendments will be presented to the governing body for discussion.