Allesley Primary School

E-Safety Policy

Reviewed: September July 2022

Next Review: July 2023

Appendices - None

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy helps to ensure safe and appropriate use. The development and implementation of such a strategy involves all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content

- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when

they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- Key e-safety messages should be reinforced as part of a planned programme of assemblies/pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Pupils should be helped to understand the need to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Rules for use of ICT systems / Internet will be posted in the ICT suite.
- Staff should act as good role models in their use of ICT, the Internet and mobile devices

Mobile Phones

Children will not need, and should not bring mobile phones into school. Mobile phones will only be allowed in exceptional circumstances by permission of the Headteacher. Permission must be sought by letter to the Headteacher, whereupon a decision will be made and the parents of the child notified.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems and online sites that the school subscribes to.
- All users will be provided with a username and password

Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Appropriate security measures are present to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Internet should always be accessed through the school's filter and appropriate security software.
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Data protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Unsuitable / inappropriate activities

Some Internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems.

The school policy restricts certain internet usage as follows:

child sexual abuse images
promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
adult material that potentially breaches the Obscene Publications Act in the UK
criminally racist material in UK
pornography
promotion of any kind of discrimination
promotion of racial or religious hatred
threatening behaviour, including promotion of physical violence or mental harm
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
Using school systems to run a private business
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
Creating or propagating computer viruses or other harmful files
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
On-line gaming (educational)
On-line gaming (non educational)
On-line gambling
On-line shopping / commerce
File sharing
Use of social networking sites
Use of video broadcasting eg Youtube

Key advice to children and young people on cyberbullying

Anti-cyberbullying code

Being sent an abusive or threatening text message, or seeing nasty comments about yourself on a website, can be really upsetting. This code gives you seven important tips to protect yourself and your friends from getting caught up in cyberbullying, and advice on to how to report it when it does happen.

1. Always respect others

Remember that when you send a message to someone, you cannot see the impact that your words or images may have on the other person. That is why it is important to always show respect to people and be careful what you say online or what images you send. What you think is a joke may really hurt someone else. Always ask permission before you take a photo of someone.

If you receive a rude or nasty message or picture about someone else, do not forward it. You could be assisting a bully and even be accused of cyberbullying yourself. You could also be breaking the law.

2. Think before you send

It is important to think before you send any images or text about yourself or someone else by email or mobile phone, or before you post information on a website. Remember that what you send can be made public very quickly and could stay online forever. Do you really want your teacher or future employer to see that photo?

3. Treat your password like your toothbrush

Don't let anyone know your passwords. It is a good idea to change them on a regular basis. Choosing hard-to-guess passwords with symbols or numbers will help stop people hacking into your account and pretending to be you. Remember to only give your mobile number or personal website address to trusted friends.

4. Block the Bully

Most responsible websites and services allow you to block or report someone who is behaving badly. Make use of these features, they are there for a reason!

5. Don't retaliate or reply

Replying to bullying messages, particularly in anger, is just what the bully wants.

6. Save the evidence

Learn how to keep records of offending messages, pictures or online conversations. These will help you demonstrate to others what is happening and can be used by your parents, school, internet service provider, mobile phone company, or even the police to investigate the cyberbullying.

7. Make sure you tell

You have a right not to be harassed and bullied online.
There are people that can help:

- Tell an adult you trust who can help you to report it to the right place, or call a helpline like ChildLine on 0800 1111 in confidence.
- Tell the provider of the service you have been bullied on (e.g. your mobile-phone operator or social-network provider). Check their websites to see where to report.
- Tell your school. Your teacher can support you and can discipline the person bullying you.

Finally, don't just stand there. If you see cyberbullying going on, support the victim and report the bullying. How would you feel if no one stood up for you?