E-Safety Policy

Last reviewed: October 2022
Next review: October 2024

E-Safety Policy

Introduction

The E-Safety Policy relates to all members of Washingborough Academy's community (including staff, governors, volunteers, contractors, pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely. It also relates to other policies including those for Computing, bullying and for Safeguarding and Child Protection.

Policy Statement

The use of digital technology is now seen as an essential part of everyday life. The number of SMS (text) messages and emails sent everyday greatly exceed the population of the planet. Nearly every company, organisation, agency, school and local authority has a presence somewhere on the internet, allowing them to engage with different people in different ways.

While digital technology can be used in positive ways, it can also be used in extremely negative ways. Paedophiles use this technology to contact, groom and blackmail young people in the virtual world with a view to abusing them in the real world, children and young people are able to anonymously bully classmates and teachers, while adults may find themselves at greater risk of identity theft should they publish too much information about their life onto a social network.

The risks are real but many people do not see that activity within a virtual world can have an effect in the real world. Comments posted onto social networking sites have led to staff being disciplined and young people being bullied. Many are also unaware that some activities in the virtual world are criminal offences and can lead to prosecution.

The Lincolnshire Safeguarding Children Board has overall statutory responsibility for the safeguarding of the child, and that includes the virtual world as well as the real, and takes seriously the role it has to ensure that member agencies co-operate to safeguard and promote the welfare of children and young people in the locality, and to ensure that they are effective in doing so.

Primarily e-Safety is used to describe pro-active methods of educating and safeguarding children and young people while they use digital technology. In order for children and young people to remain safe, we should educate them not only in the dangers but also inform them who they can contact should they feel at risk and where to go for advice while still promoting the many benefits of using digital technology, thereby empowering them with the knowledge and confidence of well researched good practice and continuing development.

The large majority of reported incidents involve children being contacted by adults for sexual purposes, visiting highly inappropriate websites or being bullied by their peers through technology. However, it should also be remembered that there have been instances where adults have been the victims through a lack of knowledge of the dangers present and by not applying real world common sense to the vast virtual world available to them on the internet.

The objective of this policy is to state a minimum standard required by Lincolnshire County Council so that schools and other establishments in Lincolnshire can build their own requirements based on own needs.

E-Safety - responsibilities of school's staff

The Headteacher has a duty of care to ensure the safety (including e-safety) of the whole school community in relation to her role with child protection. The Headteacher is also responsible for ensuring all relevant staff receives suitable training. The Headteacher will understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
The E-Safety Officer (ECO) and technician from Ark will support this role with regular monitoring and updating of firewalls, filtering and virus protection. The headteacher will work alongside the ECO to ensure a record is kept of all staff and pupils who are granted access to school ICT systems

School E-Safety Officer: Emily Spooner (Acer Class teacher)

This policy has been created with a school emphasis using the e-safety policy of Lincolnshire Safeguarding Children's Board and the Acceptable Use of ICT Policy (AUP). This is a minimum requirement to which all school staff should adhere

Internet access - You must not access or attempt to access any sites that contain any of the following:
child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues.
It is recognised that under certain circumstances inadvertent access may happen. For example, a school researching the holocaust may produce results with Nazi propaganda. Should you or a student access any of these sites unintentionally you should report the matter to a member of the Senior Management Team so that it can be logged.
Access to any of the following should be reported to Lincolnshire Police: images of child abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK.

Social networking - should be blocked in all schools until such a time where students and staff have received sufficient education in the dangers and are able to safeguard themselves online.
It is advised that Social Networking is not allowed en masse, establishments should consider which sites would be appropriate based on factors such as age range, educational value etc.
If social networking is allowed ensure that there is strict policy with regards to security of personal details, rather than relying on the default settings. You should also ensure that any age restrictions are adhered to (many social networking sites have a minimum age of 13 years). Staff should fully acquaint themselves with the privacy settings that are available on any social networking profile in order that profiles are not publicly available. Members of staff should never knowingly become "friends" with students on any social networking site or engage with pupils on internet chat.
Use of Email - All members of staff should use their professional email address for conducting school business. Use of school email for personal/social use is at the discretion of the Headteacher.

Passwords - Staff should keep passwords private. Passwords are confidential and individualised to each person. On no account should a member of staff allow a student to use a staff login.

Data Protection - Where a member of staff has to take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse, i.e. is it really necessary to take it all home, can it be encrypted, does it have to be on a USB memory stick which can be easily misplaced.

File sharing - technology such as peer to peer (P2P) and bit torrents is not permitted on the Lincolnshire School's Network.

Personal Use - Staff are not permitted to use ICT equipment for personal use unless school policy allows otherwise. If personal use is permitted, the school should emphasise what is considered within the boundaries of acceptance.

Images and Videos - Staff and pupils should not upload onto any internet site (including social media sites) images or videos of themselves or other staff or pupils without consent.

Use of Personal ICT - use of personal ICT equipment is at the discretion of the school. Any such use should be stringently checked for up to date anti-virus and malware checkers.

Viruses and other malware - any virus outbreaks are to be reported to the IT service contractor as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Staff should note that internet and email may be subject to monitoring

E-Safety Policy (pupils)

The use of ICT within schools has enormous benefits to education, however there are reasons why the school and the local authority must put some restrictions in place, such as: ICT equipment is very expensive to buy and maintain; the school and the local authority have a duty of care to ensure that you are safe and that you are not exposed to illegal or inappropriate content. It is hoped that these restrictions do not interfere with your education, but if you feel otherwise you are encouraged to talk to a member of staff to discuss any issues.

Pupils

- The school will ensure that the use of Internet derived materials by pupils acknowledges the source of information and complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be helped to understand the need for the Pupil Acceptable Use Policy, and encouraged to adopt safe and responsible use both within and outside school
- Pupils will have good role models
- Pupils will be taught what internet use is acceptable and what is not, and given clear objectives for internet use.
- 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 shown how to publish and present information to a wider audience.
- A digital literacy/online safety curriculum should be provided as part of computing/PSHE/other lessons and should be revised regularly
- Key e-safety messages should be reinforced through planned assemblies and classroom activities.
- When pupils can freely search the internet staff should monitor websites visited.

Parents will be given a copy of the pupil's acceptable use policy (AUP) and will be encouraged to support their children in following it. Parents will consult with the school if they have any concerns about their children's and others' use of technology. Parents and carers attention will be drawn to the school e-safety policy in newsletters, the school brochure and on the school website. They will promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

Many parents and guardians have limited understanding about the risks and issues of online safety. The school will endeavour to provide information and awareness to parents and guardians through:

- Curriculum activities
- Letters, newsletters and the school website/social media
- Parents evenings
- Awareness Days e.g. Safer Internet Day
- Direction to suitable websites.

Please note that internet and email use may be subject to monitoring.

Use of the Internet - the internet is provided to help you with learning activities such as research, online activities, online educational games and many other things. The internet is not to be used to access anything which is illegal, or anything that someone else may find offensive. This would include pornography, discrimination, racial or religious hatred. If you are unsure, or if you come across anything you feel is inappropriate, you should turn your computer monitor off and let your teacher know. Never try to bypass the security by using proxy sites, these are all monitored.

Social Networking - if social networking (for example Instagram, TikTok, Facebook, Twitter) is allowed in your school you should never upload pictures or videos of others without their permission. It is not advisable to upload pictures or videos of yourself, videos and pictures can easily be manipulated and used against you. You should never make negative remarks about the school or anyone within the school. Always keep your personal information private to invited friends only and never post personal information such as your full name, date of birth, address, school, phone number etc. Consider using a nickname and only inviting people you know. Universities and future employers have been known to search social networking sites before employing people.
Beware of fake profiles and people pretending to be somebody else. If something doesn't feel right, follow your instincts and report it to an appropriate adult. Never create a false profile as a joke and pretend to be somebody else, this can have serious consequences. Some social networking sites have a chat facility. You should never chat to anyone that you

don't know or don't recognise. It is recommended that you never meet a stranger after meeting them online. If you do, always inform your parents and take one of them with you.

Security - you should never try to bypass any of the security in place, this includes using proxy bypass sites. This security is in place to protect you from illegal sites, and to stop others from hacking into other people's accounts.

Copyright - you should never take information from the internet and use it as your own. A lot of information is copyright, which means that it is owned by somebody else and it is illegal to use this information without permission from the owner. If you are unsure, ask your teacher.

Etiquette - many schools provide students with email accounts, or let students post on things like blogs. Always be polite and don't swear. Consider what you are saying, and how it might be read by somebody else. Without emoticons it is difficult to show emotions in things like emails and blogs, and some things you write may be read incorrectly.

Mobile Phones - Some modern mobile phones offer the same services as a computer, i.e. Facebook, YouTube, email access etc. This can be a great way of keeping in touch with your friends and family. But, in the same way that some internet services can be used inappropriately, the same is true with mobile phones. Never take inappropriate pictures of yourself and send to your friends or upload onto social networking sites. Never forward inappropriate pictures that you have received from somebody else. In some circumstances this can be an illegal act. Your phone must be turned off and handed into the school when you arrive at school, then collected at the end of the school day before turning it back on at the school gates.

Filtering, monitoring and infrastructure

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Lincolnshire County Council can accept liability for any material accessed, or any consequences of Internet access.

- The school will work with the Ark ICT Solutions, LSB and LCC to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable online materials, the site must be reported to an adult in school who will report this to the ESL.
- All Foundation and KS1 pupils will use a class log in when using laptops and computers.
- All KS2 pupils will use an individual log in when using laptops and computers.
- All other required usernames and passwords – TTRS, Scratch, Lexia etc. will be administered by the Ark technician or the Computing lead.
- The internet is filtered for all users in school. Requests for changes need to be thoroughly checked and sent to the Ark technician.
- A procedure is in place (see pupil AUP) for pupils to report any concerns regarding technical or security issues.
- Security measures are in place to protect the school system.

Use of digital and video images (including publishing)

- Whenever a photo or video is taken it will only ever be stored on the device it was taken, the school network or the school cloud storage.
- When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose.
- Whenever a photo or video is taken/made, the member of staff will check the database before using it for any purpose.
- Any pupils shown in public materials are never identified with more than their first name.
- Staff and parents are reminded regularly about the importance of not sharing without permission.
- Members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and always moved to school storage as soon as possible and deleted from personal devices.
- Care should be taken when taking digital images/videos that pupils are appropriately dressed and are not taking part in activities that may bring the individuals or the school into disrepute.
- Video conferencing and the use of webcams should use the educational broadband network to ensure quality of service and security, if needed.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised by school staff.
- All staff will encourage pupils to think about their online reputation and digital footprint.
- Pupils will be taught about how images can be manipulated in their digital literacy curriculum.
- Pupils will be taught that they should now post images or videos of others without their permission.

Data protection and data security

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- The headteacher/principal, data protection officer and governors work together to ensure a UK GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.
- When personal data is stored on any portable computer system, memory stick or any other removable media, the device must be password protected and the data securely deleted from the device once it's use is complete.

Communications

E-mail and other communication

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will carefully monitor how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, Virtual Learning Environment etc) must be professional in tone and content.
- All parents and staff will be invited to provide a mobile telephone number(s) to receive electronic communication via Arbor.
- Only authorised staff (Head, Asistant Headteacher, School Business Manager, Senior Administrator and Administrative Assistant) will have access to Arbor.
- Parents' details will be deleted from Arbor on request, or when their child(ren) leaves the school.
- Arbor will also be used to communicate with staff and governors and relevant outside bodies as appropriate. E.g. in the event of an emergency closure.

Introducing the E-Safety policy to pupils

- Annually pupils will read, discuss and sign the Pupil AUP.
- E-Safety rules will be discussed with pupils regularly.
- The E-Safety Policy will be posted on the school website for parental benefit.
- Pupils (where appropriate) will be informed that network and Internet use will be monitored and appropriately followed up.

Personal publishing

- Parents must request permission to record e.g. video pupils at school and the school will keep a record of all such requests. Parents must only take photographs for personal use.
- Parents must not publish images/photographs/video of pupils (other than their own) or staff, or personal information about school-based events on social media sites. Any reported breaches will be subject to scrutiny and explored by the school.

Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that their image cannot be misused. Pupils' photographs will only be used if parental consent has been given.
- Pupils' full names will not be used anywhere on the school website in association with photographs.
- Written permission from parents or carers will be obtained when children join the school. Photographs of pupils will not be published on the school website without permission.
- Work can only be published with the permission of the pupil and parent/carers.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones are not permitted in school. Any necessary phone calls will be made by school staff. Year 6 to hand in mobile phones to class teacher until home time as they walk home independently.
- Nintendo DSi's, iPods, iPads and other personal games consoles systems which may have non-filtered internet connections will not be permitted in school.
- Staff will be issued with a school camera (iPad) to capture photographs of pupils.
- If 3g and 4g routers are provided for remote management to the children in extreme circumstances that all relevant filtering is in place.

Handling online safety concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding. General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Any complaint of pupil misuse, either at home or at school, must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and then reported to the ESL to take appropriate action

- We will inform parents/carers of online-safety incidents involving their children. More serious behaviour which staff or pupils may be engaged in or subject to, may involve the CEOP or/and police.

Useful websites:
CEOP is a part of the UK police force dedicated to the eradication of child sexual abuse. There is an excellent educational programme, as well as advice and videos for all ages on their website.
www.ceop.gov.uk

IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content.
www.iwf.org.uk

BBC - a fantastic resource of e-safety information for the younger child.
www.bbc.co.uk/cbbc/help/web/staysafe

Cybermentors is all about young people helping and supporting people online.
www.cybermentors.org.uk

Digital citizenship is about building safe spaces and communities, understanding how to manage personal information, and about being internet savvy - using your online presence to grow and shape your world in a safe, creative way, and inspiring others to do the same.
www.digizen.org

Inappropriate Activity flowchart