E-Safety Policy

Last reviewed: Nov 17
Next review: Nov 19

E-Safety Policy

Washingborough Academy has adopted the Lincolnshire County Council E-Safety Policy in its entirety. This policy is reproduced below.

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 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.

This policy and related guidance has been produced by LSCB, LCC and CfBT with other partner agencies in order to aid Lincolnshire schools in safeguarding children and young people from risks and dangers present in the digital world . While this policy and guidance has been produced primarily for schools the information is easily transferable in the spirit of
Integrated Children's Services.

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 schools staff

School E-Safety Officer: Katie Cropper (Blackthorn Classteacher)

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 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 Mouchel Helpdesk 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 (students)

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.

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.

Logins and Passwords - every person has a different computer login and password. You should never allow anyone else to use your details. If you think someone else may have your details you should have your password changed.

User Areas - your user area is provided for you to save school work. It is not to be used to save music or other files that you have brought in from home.

Social Networking - if social networking (for example Bebo, Facebook, Flickr) 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.
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.
If your school allows mobile phones in the classroom, these should not be used during the lesson unless your teacher has given you permission.

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.

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

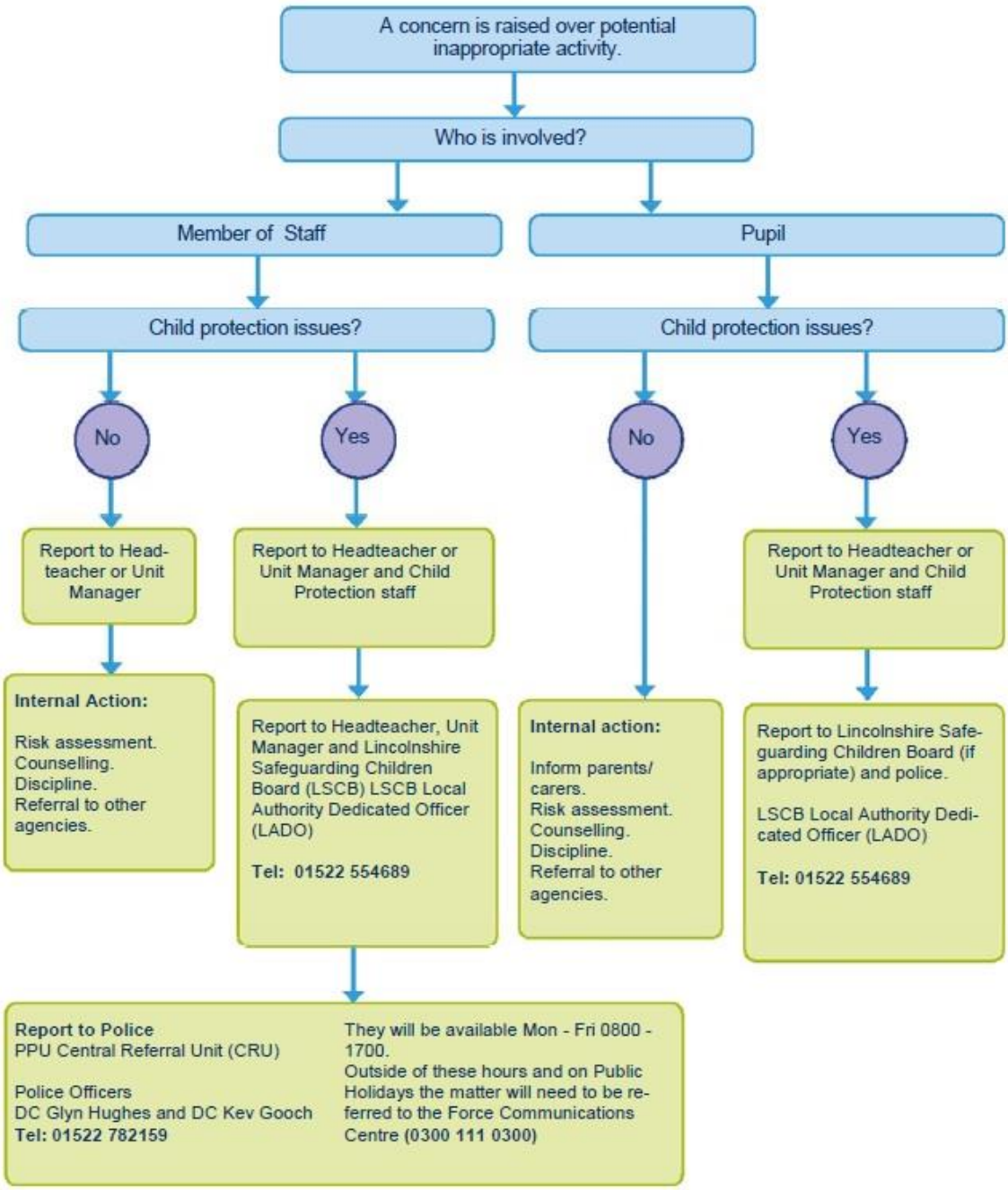
IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content.
www.iwf.org.uk

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



CfBT Education Trust

Lincolnshire COUNTY COUNCIL