Anchorsholme Academy

Online Safety Policy

Anchorsholme Academy
Online Safety Policy

Online safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Anchorsholme Academy.

As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.

Our online safety Policy has been written following current government guidance.

- The school's computing coordinators are currently **Michelle Pitt & Maxine Blundell.**
- The online safety Policy and its implementation shall be reviewed regularly by the Computing co-ordinators.
- The Governing Body at Anchorsholme Academy is ultimately responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.
- The Head teacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Computing Co-ordinators.
- The Head teacher and SLT are responsible for ensuring that the Computing Co-ordinators and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head teacher and Deputy Head should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The computing co-ordinators should take day to day-responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policy / documents and procedures including:
    - Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
    - Provide training and advice for staff.
    - Liaise with the Local Authority.
    - Liaise with school ICT technical staff.
    - Receive reports of online safety incidents and creates a log of incidents to inform future online safety developments.
    - Attend relevant meetings.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the new ICT (computing) curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, our digital footprint and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- When children are directed to websites as part of home learning they will have been checked for appropriateness by the teacher.
- Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances.

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to online safety and agree to its use:

- All staff must read and understand the contents of this policy before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access
- Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Head teacher, by recording the incident in an online safety Log. The online safety Log will be reviewed termly by one of the Computing curriculum coordinators.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

E-Mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of online safety:

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.
- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Social Networking

Social networking Internet sites (such as Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends and family over the Internet and deny access to others.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.
- Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.
- Staff will not be allowed to interact with pupils on social networking or media sites, unless it is in the context of teaching and learning.
- Staff will be encouraged not to interact with parents on social networking or media sites, unless it is in a professional context.

Use of Mobile Phones/Devices/Smart Watches etc.

Many new mobile phones/devices/smart watches have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact. The following rules must be adhered to at all times by staff, pupils and parents.

Staff

- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use a school phone to contact parents.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom, whilst pupils are present.
- Staff may use their mobile phones in the staffroom/classrooms when pupils aren't present during the lunch period or at break times.
- Mobile phones or other similar devices should be switched onto silent during the school day.

Pupils

- The sending of abusive or inappropriate text messages is forbidden.
- If a pupil brings a mobile phone or similar device into school, it must be left at the school office and collected at the end of the day.

Parents

- The sending of abusive or inappropriate text messages is forbidden whilst on school property.
- Parents cannot use mobile phones on school trips to take pictures of the children.

Digital/Video Cameras

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents will not use digital cameras, mobile phones or video equipment at school unless specifically authorised by staff.
- The Head teacher or nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.

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.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- The Head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and individual pupils will not be published where the appropriate parent or guardian has not given their permission.
- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Web site.
- Parents may upload pictures of their own child only onto social networking sites. If the picture includes another child / children then it is their responsibility to gain permission from that child's parents.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority where necessary.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act. 14.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate.

Handling online safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher
- Discussions will be held with the local police to establish procedures for handling potentially illegal issues.

Communication of Policy Pupils

- Rules for Internet access will be posted in the Computing room.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be regularly informed about the importance of being safe on social networking sites.
- All staff will have access to the School online 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

- Parents' attention will be regularly drawn to the School online safety Policy in newsletters and on the school Website.

Further Resources:

We have found these web sites useful for online safety advice and information.
http://www.thinkuknow.co.uk/ set up by the Police with lots of information for parents and staff including a place to report abuse.
http://www.childnet-int.org/ Non-profit organisation working with others to "help make the Internet a great and safe place for children".

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/
Becta
http://schools.becta.org.uk/index.php?section=is
Chat Danger
www.chatdanger.com/
Child Exploitation and Online Protection Centre
www.ceop.gov.uk/
Childnet
www.childnet-int.org/
Digizen
www.digizen.org/
Lancashire e-Safety Policy and Guidance, Posters etc
www.lancsngfl.ac.uk
Kidsmart
www.kidsmart.org.uk/
Lancashire Police – online-Safety
www.lancashire.police.uk/need-to-know/about-how-to-stay-safe/on-the-web
Safer Children in the Digital World www.dfes.gov.uk/byronreview/

Useful resources for Parents

Parenting in the digital age
http://www.pitda.co.uk/
Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk
Children, ICT & e-Safety (Keeping children safe in the Digital World)
www.lancsngfl.ac.uk/esafety/index.php?category_id=10
www.kented.org.uk/ngfl/ict/safety.htm
Parents CentreParents Centre
www.parentscentre.gov.uk
Internet Safety Zone
www.internetsafetyzone.com

Anchorsholme Academy website: http://www.anchorsholme.co.uk/

Guidance for this policy was taken from Lancashire Online-safety policy document 2013
http://www.lancsngfl.ac.uk/esafety/download/file/Final%20version%20eSafety_Guidance_Document_February2013.pdf

Appendices.

Appendix 1: Online safety Audit.

This ANNUAL self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy.

All staff could contribute to the audit including: Designated Child Protection Coordinator, SENCO, online-Safety Coordinator, Network Manager and Head teacher.
Date of latest update (at least annual):

The school online safety policy was agreed by governors on:

The policy is available for staff at:

The policy is available for parents/carers at:

The responsible member of the Senior Leadership Team is:

The responsible member of the Governing Body is:

The Designated Child Protection Coordinator is:

The online safety Coordinator is:

Details of Check		Details of action required.
Has the school an online safety Policy that complies with Lancashire guidance?	Y/N	
Has online safety training been provided for both pupils and staff?	Y/N	
Is there a clear procedure for a response to an incident of concern?	Y/N	
Have online safety materials from CEOP and Becta been obtained?	Y/N	
Do all staff sign a Code of Conduct for ICT on appointment?	Y/N	
Are all pupils aware of the School's online Safety Rules?	Y/N	
Are online safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y/N	
Do parents/carers sign and return an agreement that their child will comply with the School online Safety Rules?	Y/N	
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N	
Has an ICT security audit been initiated by SLT, possibly using external expertise?	Y/N	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N	
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements (e.g. Lancashire Cumbria, Regional Broadband Consortium, NEN Network)?	Y/N	
Has the school-level filtering been designed to reflect educational objectives and approved by SLT?	Y/N	

Appendix 2 Online -Safety Incident Log

All online safety incidents must be recorded.

This incident log will be monitored and reviewed regularly by the Head teacher and Chair of Governors.

Date & time of incident.	Type of incident.	Name of pupils and staff involved.	System details.	Incident details.	Resulting actions taken and by whom.

Appendix 3: ICT Acceptable Use Policy (AUP) – Staff and Governors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school.

This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology.

All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the head teacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in online-Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not use the school system(s) for personal use during working hours.
9. I will not install any hardware or software without the prior permission of: G. Dow, A. Hurley, K. Proctor, M. Pitt or M. Blundell
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult.
12. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
13. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
14. I will report any known misuses of technology, including the unacceptable behaviours of others.
15. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
16. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
17. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to

access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

18. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
19. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
20. I will take responsibility for reading and upholding the standards laid out in the AUP.
21. I will support and promote the school's online-Safety policy and help children to be safe and responsible in their use of ICT and related technologies.
22. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..…….....……..

Date …….…….....……..

Full Name …….....…..… (PRINT)

Position/Role …….....…….

Appendix 4: Acceptable Use Policy (AUP) – Children.

These rules reflect the content of our school's online safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren).

- I will only use ICT in school for school purposes.
- I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will only use my class e-mail address or my own school email address when emailing.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in inappropriate electronic materials from home.
- I will not deliberately look for, or access inappropriate websites.
- If I accidentally find anything inappropriate I will tell my teacher immediately.
- I will only communicate online with people a trusted adult has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others', details such as names, phone numbers or home addresses.
- I will not tell other people my ICT passwords.
- I will not arrange to meet anyone that I have met online.
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my online-Safety.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

……Parent/ Carer Signature

We have discussed this Acceptable Use Policy and

……..... [Print child's name] agrees to follow the online-Safety rules and to support the safe use of ICT at Anchorsholme Academy.

Parent /Carer Name (Print) ……..…….

Parent /Carer (Signature) ……..……. ……..

Class …….

Date……..…….

This AUP must be signed and returned before any access to school systems is allowed.

Appendix 5: ICT Acceptable Use Policy (AUP) – Example Parent's Letter

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate.

This is particularly relevant when using Social Network Sites that incorporate age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School online safety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible.

Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school. If you would like to find out more about online-Safety for parents and carers, please visit the Lancashire online safety website at http://www.lancsngfl.ac.uk/esafety

If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact

Yours sincerely,

Head teacher.

Appendix 6: Online safety rules poster EYFS/KS1

Online Safety Rules.

Our Golden Rules for Staying Safe with Computing.

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

We always ask a trusted adult if we need help using the Internet.

We always tell a trusted adult if we find something that upsets us.

EYFS/KS1

Appendix 7: Online safety rules poster KS2

Online Safety Rules.

Our Golden Rules for Staying Safe with ICT.

We always ask permission before using the internet.

We only use the Internet when a trusted adult is around.

We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).

We always tell an adult if we see anything we are uncomfortable with.

We only communicate online with people a trusted adult has approved.

All our online communications are polite and friendly.

We never give out our own, or others', personal information or passwords and are very careful with the information that we share online.

We only use programmes and content which have been installed by the school.

KS2