Ashton Community Science College

Online Safety Policy

Version Control

Named Owner:	Ms C Parkinson (Associate Assistant Headteacher)
Version Number:	1.00
Date Of Creation:	
Last Review:	April 2020
Next Scheduled Review:	April 2023
Overview of Amendments to this Version:	To be reviewed alongside Safeguarding and Addressing Bullying policies

1. Aims

Ashton Community Science College aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is John Swindells
All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead and Deputy DSL are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that students follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum.

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
-

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website.This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers and form teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Students using mobile devices in school

Students may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Form time
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and Deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This can be found on CPOMS.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1: acceptable use agreement (students and parents/carers)

Dear Parents/Carers

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, Ashton Community Science College is providing supervised access to the Internet and e-mail. We believe that the use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached 'Network, E-mail and Internet Use Good Practice - 'Rules for ICT Use' document, and sign and return the consent form so that your child may use the network and Internet at school.

There have been concerns about students having access to undesirable materials. Please be assured, we take positive steps to deal with this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we can provide references to information on safe Internet access if you wish. We also have leaflets from national bodies that explain the issues further.

Whilst every effort is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Thank you for your support in this matter.

Yours sincerely

Miss S Asquith
Headteacher

Network, E-mail and Internet Use

Rules for ICT Users

The school computer system provides an enhanced learning experience through access to the Internet and e-mail. It is important to remember that this access is a privilege, not a right, and comes with it responsibilities for all involved. The following will help protect students and the school by clearly stating what is and is not acceptable.

- School computer and Internet use must be appropriate to the student's education.
- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- Users must take reasonable precautions to ensure no computer viruses are introduced to the network, when transferring school work from portable storage devices
- Copyright and intellectual property rights must be respected.
- Users must respect the work of others, which might be stored in common areas on the system. Conversely, users should always try and store their files and data in their own secure area or on removable media. Files and data stored in common areas of the system must be transferred at the earliest opportunity to the users own area. Such files will be regularly removed from the system. Games are not allowed to be saved in user areas or common areas.
- Users are responsible for any e-mails they send, any postings they make to forums. Both should be written carefully and politely. As messages may be forwarded and postings will be read by other students and staff, they are best regarded as public property. Anonymous messages and chain letters must not be sent.
- Users should report any unpleasant material or messages received. The report will be confidential and will help protect others.
- The use of public chat rooms is not allowed.
- The school ICT systems may not be used for private business purposes, unless the Principal has given permission for that use. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in the loss of Internet access.
- Any faults with I.T. equipment must be reported to a member of staff.
- Users must take care of I.T. equipment and surrounding workstation.
- No food or drink is to be consumed whilst in the vicinity of I.T. Equipment.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites and postings to forums, the interception of e-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unsuitable, unauthorised or unlawful.

Cyber Bullying – Code of Conduct

- If you feel you are being bullied by email, text or online within school, contact a member of staff.
- Never send any bullying or threatening messages. Anything you write and send could be read by an adult.
- Serious bullying should be reported to the police - for example threats of a physical or sexual nature.
- Keep and save any bullying emails, text messages or images.
- If you can, make a note of the time and date bullying messages or images were sent, and note any details about the sender.
- Why not log into a chat-room with a different user ID or nickname? That way the bully won't know who you are. You could change your mobile phone number and only give it out to close friends.
- Contact the service provider (mobile phone company, your internet provider) to tell them about the bullying. They may be able to track the bully down.
- Use blocking software - you can block instant messages from certain people or use mail filters to block emails from specific email addresses.
- **Don't** reply to bullying or threatening text messages or emails- this could make matters worse. It also lets the bullying people know that they have found a 'live' phone number or email address. They may get bored quite quickly if you ignore them.
- **Don't** give out your personal details online - if you're in a chat-room, watch what you say about where you live, the school you go to, your email address etc. All these things can help someone who wants to harm you build up a picture about you.
- **Don't** forward abusive texts or emails or images to anyone. You could be breaking the law just by forwarding them. If they are about you, keep them as evidence. If they are about someone else, delete them and don't reply to the sender.
- **Don't** ever give out passwords to your mobile or email account.
- **Remember** that sending abusive or threatening messages is against the law.

Adapted from Anti Bullying Network
http://www.antibullying.net/

Consent Form
For Students

Ashton Community Science College **Responsible Network, E-mail and Internet Use** Please complete, sign and return to the Headteacher	
Student:	Form:
Student's Agreement I have read and understand the school 'Network, E-mail and Internet Use - Rules for ICT Users' document. I will use the computer system and Internet in a responsible way and adhere to these rules at all times.	
Signed:	Date:
Parent / Carer's Consent for Internet Access I have read and understood the school 'Network, E-mail and Internet Use- Rules for ICT Users' document and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.	
Signed:	Date:
Please print name:	

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Network, E-mail and Internet Use Good Practice
Rules for ICT Use

The school computer system provides Internet access to staff for teaching and learning. This Network, E-mail and Internet Use Good Practice statement will help protect staff and the school by clearly stating what is acceptable and what is not.

- School computer and Internet use must be appropriate for work purposes.
- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- Users must take reasonable precautions to ensure no computer viruses are introduced to the network, when transferring school work from portable storage devices
- Copyright and intellectual property rights must be respected.
- E-safety should be promoted with students when using the ICT facilities, to help them develop a responsible attitude to using ICT both in and out of school.
- Users must respect the work of others, which might be stored in common areas on the system. Conversely, users should always try and store their files and data in their own secure area or on removable media. Files and data stored in common areas of the system must be transferred at the earliest opportunity to the user's own area. Such files will be regularly removed from the system.
- Users are responsible for e-mail they send and for contacts made. E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property. Anonymous messages and chain letters must not be sent.
- Users should report any unpleasant material or messages received. The report will be confidential and will help protect others.
- The use of public chat rooms is not allowed.
- The school ICT systems may not be used for private business purposes, unless the Headteacher has given permission for that use. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in the loss of Internet access.
- Any faults with I.T. Equipment must be reported to the Technical Support Department
- Users must take care of I.T. Equipment and surrounding workstation
- No food or drink is to be consumed whilst in the vicinity of I.T. Equipment
- Use of the Internet for personal/private reasons during lessons/ student contact time is not acceptable

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful, The SLT and/or network manager may access employees' emails if it is deemed necessary for the daily operations of the school.

Consent Form

Staff and Third-Party Use

Ashton Community Science College **Responsible Network, E-mail and Internet Use** Please complete, sign and return to the ICT Support Department	
Name:	Department:
Agreement I have read and understand the school 'Network, E-mail and Internet Use Good Practice - Rules for ICT Users' document. I will use the computer system and Internet in a responsible way and obey these rules at all times.	
Signed:	Date:

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	