ASTREA ACADEMY
DEARNE
Astrea Academy Trust
INSPIRING BEYOND MEASURE

Online Safety Policy

Policy review date	12.11.2023
Next review date	12.11.2024

1. Introduction

1.1 The purpose of this policy is to establish the rules within the academy for using ICT equipment and the Internet. Please also refer to Safer Working Practices 2015 (Astrea Academy Dearne School Code of Conduct), Safeguarding and Child Protection Policy and Positive Relationships and Behaviour Policy.

1.2 The National Online Safety Hub (2022) states *"online safety is the act of staying safe online"* and that it *"encompasses all technological devices which have access to the internet from PCs and laptops to smartphones and tablets."*

1.3 New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/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.

2. Aim

2.1 The aim of the online safety policy is to ensure staff and students use devices safely and appropriately.

2.2 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 as they may face dangers such as;

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- 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.

2.3 The issues that are classified within Online Safety is considerable and ever evolving. However, it can be categorised in to the four areas of risk. These areas form the process of how to the academy takes action to protect children from dangers online.

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying
Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org)

2.4 Many of these risks reflect situations in the off-line world and it is essential that this online policy is read and used in conjunction with other school policies specifically, Behaviour, Child Protection and Mobile Phone Use.

2.5 As with all other risks, it is impossible to eliminate those risks completely. It is therefore vitally important, through good educational provision, to build pupils' knowledge and resilience to the risks to which they may be exposed, so that they have the confidence and knowledge to face and deal with them.

2.6 The school does provide the necessary safeguards to ensure that everything that could reasonably be expected to manage and reduce these risks has been done. The Online Safety policy explains how the school intends to do this, simultaneously addressing wider educational which should help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

3. Scope

3.1 This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers Principals, to such an extent considered reasonable, to regulate the behaviour of 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 Online Safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

3.2 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 Online Safety behaviour that take place out of school.

4. Principal & Senior Leadership Team

The Principal is responsible for ensuring:

4.1 The safety (including Online Safety) of all members of the school community,
4.2 Adequate training
4.3 Effective monitoring systems are set up, reviewed and monitored
4.4 A relevant reporting procedure so online safety concerns are understood by all staff
4.5 The establishment and review of the school Online Safety policies and documents (in conjunction with Online Safety coordinator).
4.6 Training of the school's Designated Safeguarding Lead and all deputies in Online Safety so they are aware of potential serious child protection issues which may arise through the use of ICT.

5. Designated Safeguard Leader

The Designated Safeguard Leader takes day to day responsibility for rectifying any Online Safety issues and has a leading role in:

5.1 Liaising with Staff, the LA, ICT Technical Staff, Safeguarding Governor and SLT on all issues related to Online Safety;
5.2 Ensuring that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place;
5.3 Providing training and advice for staff;
5.4 Receiving reports of Online Safety incidents through the Safeguarding Software CPOMS, reviewing these incidents to inform future Online Safety developments
5.5 Co-ordinating and reviewing the Online Safety education programme in school

6. Astrea Managed Service

The Astrea Managed Service is responsible for ensuring that:

6.1 The school's ICT infrastructure is secure and meets Online Safety technical requirements
6.2 The school's password policy is adhered to
6.3 The school's monitoring and filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
6.4 The use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can and should be reported to the Designated team for safeguarding and SLT for investigation/action/sanction.

7. Teaching & Support Staff

In addition to elements covered in the Staff Accessible Usage Policy (AUP), all teaching and support staff are responsible for ensuring that:

7.1 They have an up-to-date awareness of Online Safety through required training and also have an awareness of online safety policy and practices, for example knowing how to report a concern

7.2 They have read, understood and signed the school Staff Acceptable Usage Policy (AUP)

7.3 Online Safety issues are embedded in all aspects of the curriculum and other school activities

7.4 Students understand and follow the school's Online Safety and acceptable usage policies

7.5 Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

7.6 They monitor ICT activity in lessons, extracurricular and extended school activities

7.7 In lessons where internet use is pre-planned, 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.

8. Students (to an age-appropriate level)

8.1 Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be provided with a copy of the policy. This will be sent home via email or postal service.

8.2 Will need to agree to the Acceptable Use Policy before they login in to a device. This is shown when student logs in to the network for the first time.

8.3 Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

8.4 Should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety policy also covers their actions out of school, if related to their membership of the school.

9. Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

9.1 Endorsing (by signature) the Pupil Acceptable Usage Policy.

9.2 Accessing the school website in accordance with the relevant school Acceptable Usage Policy.

9.3 Reporting any instances of any inappropriate use of Online Safety

9.4 Using the dedicated academy webpage to report any instance

10. Community Users

Community Users who access school ICT systems/website/Learning Platform as part of the Extended School provision will be expected to sign a Volunteer User AUP (see Appendix 6) before being provided with access to school systems.

11. Education and Training

Online Safety education will be provided in the following ways:

11.1 The provision on an online safety programme is provided as part of the form tutor and spinal assembly programme. This will be regularly revisited in ICT and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school.

11.2 Students taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.

11.3 Students helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside of school.

11.4 Students taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

11.5 Staff act as good role models with their use of ICT, the internet and mobile devices.

12. Acceptable Usage Policy

12.1 Parents/Carers will be provided with a copy of the student Acceptable Use Policy

12.2 Staff are required to complete an Academy Trust Acceptable Use Policy that they must read through and sign to indicate understanding of the rules.

12.3 students will complete an acceptable use policy when they logon to a device within the academy for the first time.

13. Copyright

13.1 Students to be taught the skills appropriate to search and use the internet for research and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this.

13.2 Students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

14. Communication

Email

14.1 Digital communications with pupils (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official school systems (see staff guidance in child protection policy).

14.2 The school's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, school curriculum systems);

14.3 Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses.

14.4 School e-mail is not to be used for personal use. Staff can use their own email in school (before, after school and during lunchtimes when not working with children) – but not for contact with parents/ pupils.

15. **Mobile Phones and Smart Devices**

15.1 **Only School** mobile phones, should be used to contact parents/carers/students when on school business with students off site. Staff should not use personal mobile devices.

15.2 **Staff** should not be using personal mobile phones in school during working hours when in contact with children

15.3 **Staff** should only use mobile phones in designated areas, outlined in the Positive Relationships and Behaviour Policy

15.4 **Students** should adhere to the rules and guidelines set out in the Behaviour Policy regarding mobile phone and smart device use in school. Please click here to see Positive Relationships and Behaviour Policy

16. Social Networking Sites

Young people will not be allowed on social networking sites at school. At home it is the responsibility of parents to monitor their child's use of social networking sites and should be aware that many popular sites have a minimum age of 13.

16.1 **Staff** should not access social networking sites for personal reasons on school equipment in school or at home. Staff should access sites using personal equipment.

16.2 **Staff** users should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site or blog**.**

16.3 Staff using social media networking sites for professional reasons are reminded to remain professional in that they will not contain images of their own family members or any personal details

16.4 **Students/Parents/carers** should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.

16.5 If inappropriate comments are placed on social networking sites about the school or school staff then advice will be sought from the relevant agencies, including the police if necessary.

16.6 Students will be taught about Online Safety on social networking sites as we accept some may use it outside of school.

17. Digital Images

17.1 The school record of parental permissions granted/not granted must be adhered to when taking images of our students. All information is stored on BROMCOM.

17.2 Under no circumstances should images be taken using privately owned equipment without the express permission of the Principal or the Online Safety Coordinator.

17.3 Where permission is granted the images should be transferred to school storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has an active website and Twitter account which are used to inform and publicise school events and celebrate and share the achievement of students.

18. Removable Data Storage Devices

18.1 Students should not bring their own removable data storage devices into school unless asked to do so by a member of staff.

18.2 Staff must gain permission of the Principal or Network Manager to use removable data storage devices

19. Websites

In lessons where Internet use is pre-planned, students 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.

19.1 Staff will preview any recommended sites before use.

19.2 Staff will be discouraged not to use open searches with younger students for example, "finding images/ information on...") who may misinterpret information.

19.3 If internet research is set for homework, specific sites will be suggested that have previously been checked by staff. **Parents** will be advised to supervise any further research.

19.4 Teachers will carry out a risk assessment regarding which students are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the students on the internet by the member of staff setting the task. All staff are aware that if they pass students working on the internet that they have a role in checking what is being viewed. Students are also aware that all internet use at school is tracked and logged.

19.5 The school allows the Designated Safeguarding leaders, Online Safety Co-ordinator, Network Manager and SLT to access to Internet logs.

20. Passwords and Encryption

Staff

20.1 Passwords or encryption keys should not be recorded on paper or in an unprotected file

20.2 Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

Students

20.3 Should only let school staff know in-school passwords.

20.4 Inform staff immediately if passwords are traced or forgotten.

20.5 IT technicians and designated teachers are able to access the network to allow students to change passwords.

21. Use of Own Equipment

21.1 Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Principal or Network Manager.

21.2 Students should not bring in their own equipment unless asked to do so by a member of staff.

22. Use of School Equipment

22.1 No personally owned applications or software packages should be installed on to school ICT equipment;

22.2 Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.

22.3 All staff and students should ensure any screens are locked (by pressing Alt, Ctrl & Delete simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

23. Filtering and Monitoring

All use of the school's internet access is monitored and the logs are randomly but regularly monitored by the school IT staff. Whenever any inappropriate use is detected it will be recorded timely on CPOMS and it will be followed up by the Pastoral & Safeguarding Team or members of the Senior Leadership Team.

23.1 A review on how effective the school filters and monitoring systems are will take place annually by member of the Senior Leadership Team, the Designated Safeguard Lead, and IT services within the academy.

The academy will ensure that the Leadership Team and relevant staff are:

- Aware of and understand the systems in place
- Manage them effectively
- Know how to escalate concerns when identified.

23.2 The academy share information with parents/careers about:

- What systems are in place to filter and monitor online use
- What websites children will be asked to access
- Who (if anyone) children will be interacting with online.

23.1 **Incident Reporting**

Any Online Safety incidents must immediately be reported to the Principal (if a member of staff) or the Designated Safeguard lead (if a student) who will investigate further following Online Safety and safeguarding policies and guidance.

23.2 **23.2 Responding to incidents of misuse**

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. Listed in Appendix 2 are the responses that will be made to any apparent or actual incidents of misuse. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the flow chart should be consulted. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows (Appendix 3 for students and Appendix 4 for staff respectively).

Appendix 1

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

		Staff and other adults					Students and young people			
Communication Technologies		Permitted	Permitted at certain times	Permitted for named staff	Not Permitted		Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones May be brought to school		X					X			
Mobile phones used in lessons			X							X
Use of mobile phones in social time		X								X
Taking photographs on mobile devices				X						X
Use of PDAs and other educational mobile devices		X					X			
Use of school email for personal emails					X					X
Social use of chat rooms/facilities					X					X
Use of social network sites				X						X
Use of educational blogs		X					X			

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 students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person (in accordance with the school policy) 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, Learning Platform etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal

email addresses, text messaging or public chat/social networking programmes must not be used for these communications.

- Students 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.

Appendix 2

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, as defined below, 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. Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					X
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
Obscene publications or malicious communications					X
Criminally racist material in the UK					X
Pornography				X	
Promotion of any kind of discrimination				X	
Promotion of racial or religious hatred					X
Threatening behaviour, including promotion of physical violence or mental harm					X
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				X	
Using school systems to run a private business				X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
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				X	
On-line gaming (educational)		X			
On-line gaming (non- educational)				X	
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social networking sites			X		
Downloading video broadcasting e.g. Youtube	X				
Uploading to video broadcast e.g. Youtube			X		

Appendix 3

Incident involving students	**Teacher to use school behaviour policy to deal with**	**Refer CPOMS** **Monitored by pastoral and safeguarding team**	**Refer to Police**	**Refer to technical support staff for action re security/filtering etc**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities**).**		X	X	X
Unauthorised use of non-educational sites during lessons	X			X
Unauthorised use of mobile phone/ digital camera/ other handheld device.	X			
Unauthorised use of social networking/ instant messaging/ personal email	X	X		X
Unauthorised downloading or uploading of files		X		X

Allowing others to access school network by sharing username and passwords		X		X
Attempting to access or accessing the school network, using another student's account		X		X
Attempting to access or accessing the school network, using the account of a member of staff		X		X
Corrupting or destroying the data of other users		X		X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X		X
Continued infringements of the above, following previous		X	Community Police Officer referral	X

warnings or sanctions				
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X
Using proxy sites or other means to subvert the school’s filtering system		X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X		X

The guidance in this policy should be implemented with cross reference to the School’s Child Protection, Anti-Bullying and Behaviour Policies. Note, attempts have been made to synchronise guidance and sanctions.

Appendix 4

Incidents involving members of staff	**Refer to the Principal** **In event of breaches of policy by the Principal, refer to the Chair of Governors**	**Refer to technical support staff for action re filtering, security etc**	**Referral to AAT and LADO** **Potential Disciplinary Action**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	X	X	X

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X		X
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	X	X	X
Unauthorised downloading or uploading of files	X	X	X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person’s account.	X	X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X		X
Deliberate actions to breach data protection or network security rules	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ pupils	X	X	X
Actions which could compromise the staff member’s professional standing	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X
Using proxy sites or other means to subvert the school’s filtering system	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X
Breaching copyright or licensing regulations	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X		X